paloalto TECHDOCS

Panorama 관리자 안내서

Version 11.1



docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 9, 2024

Table of Contents

Panorama 개요 11

Panorama 정보 12
Panorama 모델 14
중앙 집중식 방화벽 구성 및 업데이트 관리 17
- 컨텍스트 스위치 - 방화벽 또는 Panorama 17
- Panorama의 총 구성 크기 18
- 템플릿 및 템플릿 스택(template stack) 18
- 디바이스 그룹 20

중앙 집중식 로깅 및 보고 25
- 관리형 수집기 및 수집기 그룹 25
- 로컬 및 분산 로그 수집 26
- 여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항 27
- 로그 포워딩 옵션 29
- 중앙 집중식 보고 30

Panorama를 사용한 데이터 재배포 31
역할 기반 액세스 제어 32
- 관리 역할 32
- 인증 프로필 및 시퀀스 34
- 액세스 도메인 34
- 관리 인증 35

Panorama 커밋, 검증 및 미리보기 작업 37
Panorama 배포 계획 39
Panorama 배포: 작업 개요 41

Panorama 설정 43

Panorama 로그 스토리지 요구 사항 결정 44
대규모 방화벽 배포 관리 47
- 최적의 대규모 방화벽 배포 솔루션 결정 47
- M-시리즈 및 Panorama 가상 어플라이언스를 위한 디바이스 관리 용량 증가 47

Panorama 가상 어플라이언스 설정 51
- Panorama 가상 어플라이언스의 전제 조건 설정 51
- Panorama 가상 어플라이언스 설치 56
- Panorama 가상 어플라이언스의 초기 구성 수행 118
- Panorama 가상 어플라이언스를 로그 수집기로 설정 122
- 로컬 로그 수집기로 Panorama 가상 어플라이언스 설정 130
- Panorama 모드에서 Panorama 가상 어플라이언스 설정 136
- 관리 전용 모드에서 Panorama 가상 어플라이언스 설정 136

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스에서 로그 스토리지 용량 확장 137
Panorama 가상 어플라이언스에서 CPU 및 메모리 늘리기 164
Panorama 가상 어플라이언스의 시스템 디스크 늘리기 171
Panorama 가상 어플라이언스 설정 완료 177
Panorama 가상 어플라이언스 변환 177
M-시리즈 어플라이언스 설정 189
M-시리즈 어플라이언스 인터페이스 189
M-시리즈 어플라이언스의 초기 구성 수행 191
에어 갭 M-Series 어플라이언스의 초기 구성 수행 196
M-시리즈 설정 개요 200
M-시리즈 어플라이언스를 로그 수집기로 설정 202
M 시리즈 어플라이언스의 스토리지 늘리기 212
다중 인터페이스를 사용하도록 Panorama 구성 218
Panorama 등록 및 라이선스 설치 225
Panorama 등록 225
Panorama 지원 라이선스 활성화 227
Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색 228
Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스 활성화/검색 229
M-시리즈 어플라이언스에서 방화벽 관리 라이선스 활성화/검색 231
Panorama 디바이스 인증서 설치 234
전용 로그 수집기에 대한 디바이스 인증서 설치 237
다른 Panorama 모델로 전환 240
Panorama 가상 어플라이언스에서 M 시리즈 어플라이언스로 마이그레이션 240
Panorama 가상 어플라이언스를 다른 하이퍼바이저로 마이그레이션 244
M 시리즈 어플라이언스에서 Panorama 가상 어플라이언스로 마이그레이션 249
M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션 256
M-100 또는 M-500 어플라이언스에서 M-200 또는 M-600 어플라이언스로 마이그레이션 259
Panorama 관리 인터페이스 액세스 및 탐색 264
Panorama 웹 인터페이스에 로그인 264
Panorama 웹 인터페이스 탐색 265
Panorama CLI에 로그인 265
Panorama에 대한 관리 액세스 설정 267
관리자 역할 프로파일 구성 267
관리형 방화벽에 대한 선택적 푸시를 위한 관리자 역할 프로파일 구성 268
액세스 도메인 구성 269
관리 계정 및 인증 구성 270

 ©2024 Palo Alto Networks, Inc.

관리자에 대해 SCP 업로드 활성화 283
관리자 활동 추적 구성 287
사용자 지정 인증서를 사용하여 인증 설정 290
SSL/TLS 연결은 어떻게 상호 인증됩니까? 290
Panorama에서 사용자 지정 인증서를 사용하여 인증 구성 291
관리되는 디바이스에서 사용자 지정 인증서를 사용하여 인증 구성 293
새 클라이언트 디바이스 추가 295
인증서 변경 295

방화벽 관리 299
관리되는 디바이스로 방화벽 추가 300
관리 방화벽에 대한 디바이스 인증서 설치 308
관리 방화벽에 대한 디바이스 인증서 설치 308
디바이스 인증서가 없는 모든 관리형 방화벽에 대한 디바이스 인증서 설치 312
Panorama 관리와 클라우드 관리 간의 변경 사항 317
Panorama 관리에서 클라우드 관리로 변경 317
클라우드 관리에서 Panorama 관리로 변경 317
제로 터치 프로비저닝 설정 319
ZTP 개요 319
ZTP 플러그인 설치 321
ZTP 설치 관리자 계정 구성 329
Panorama에 ZTP 방화벽 추가 330
ZTP 작업에 CLI 사용 343
ZTP 플러그인 제거 346
디바이스 그룹 관리 348
디바이스 그룹 추가 348
디바이스 그룹 계층 생성 349
공유 또는 디바이스 그룹 정책에서 사용할 개체 생성 351
상속된 개체 값으로 되돌리기 353
미사용 공유 객체 관리 353
상속된 개체의 우선 순위 관리 354
정책 규칙 또는 다른 디바이스 그룹으로 이동 또는 복제 355
방화벽의 하위 집합에 정책 규칙 푸시 356
Multi-VSYS 방화벽으로 디바이스 그룹 푸시 359
규칙 계층 구조 관리 360
템플릿 및 템플릿 스택(template stack) 관리 362
템플릿 기능 및 예외 362
템플릿 추가 362
템플릿 스택(template stack) 구성 365

 ©2024 Palo Alto Networks, Inc.

템플릿 또는 템플릿 스택(template stack) 변수 구성 369
기존 템플릿 스택(template stack) 변수 가져오기 및 덮어쓰기 372
템플릿 또는 템플릿 스택(template stack) 값 재정의 374
템플릿 설정 비활성화/제거 376
Panorama에서 마스터 키 관리 377
관리되는 방화벽에 대한 구성 푸시 예약 383
관리되는 방화벽에 데이터 재분배 386
방화벽을 Panorama 관리로 전환 389
Panorama 관리로의 전환 계획 389
방화벽을 Panorama 관리로 마이그레이션하고 기존 구성 재사용 390
방화벽을 Panorama 관리로 마이그레이션하고 새 구성 푸시 394
방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성 재사용 397
방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성 푸시 401
부분 방화벽 구성을 Panorama에 로드 403
관리되는 방화벽에서 Panorama 푸시 구성 현지화 406
Panorama 디바이스 모니터링 409
디바이스 상태 모니터링 409
정책 규칙 사용 모니터링 411
사용 사례: Panorama를 사용하여 방화벽 구성 418
이 사용 사례의 디바이스 그룹 418
이 사용 사례의 템플릿 419
중앙 집중식 구성 및 정책 설정 420

로그 수집 관리 427
관리형 수집기 구성 428
관리형 수집기 상태 모니터링 435
전용 로그 수집기에 대한 인증 구성 436
전용 로그 수집기에 대한 관리 계정 구성 436
전용 로그 수집기에 대한 RADIUS 인증 구성 438
전용 로그 수집기에 대한 TACACS+ 인증 구성 441
전용 로그 수집기에 대한 LDAP 인증 구성 444
수집기 그룹 관리 449
수집기 그룹 구성 449
로그 수집기 간에 사용자 지정 인증서로 인증 구성 452
로그 수집기를 다른 수집기 그룹으로 이동 454
수집기 그룹에서 방화벽 제거 455
Panorama에 대한 로그 포워딩 구성 456
외부 대상에 대한 Syslog 포워딩 구성 460
로그를 Strata Logging Service로 포워딩 464

 ©2024 Palo Alto Networks, Inc.

Panorama로 로그 포워딩 확인 465
로그 포워딩 및 버퍼링 기본값 수정 466
Panorama에서 외부 대상으로 로그 포워딩 구성 468
로그 수집 배포 471
전용 로그 수집기로 Panorama 배포 471
로컬 로그 수집기가 있는 Panorama M-시리즈 어플라이언스 배포 480
로컬 로그 수집기로 Panorama 가상 어플라이언스 배포 486
로컬 로그 수집을 사용하여 레거시 모드에서 Panorama 가상 어플라이언스 배포 491

Manage WildFire Appliances 495
Panorama로 관리할 독립형 WildFire 어플라이언스 추가 496
Panorama에서 기본 WildFire 기기 설정 구성 501
WildFire 어플라이언스에 대한 인증 구성 501
WildFire 어플라이언스 및 클러스터에서 사용자 지정 인증서를 사용하여 인증 설정 514
Panorama Managed WildFire 어플라이언스에 대한 사용자 지정 인증서 구성 514
WildFire 클러스터에 대한 단일 사용자 지정 인증서로 인증 구성 516
Panorama를 통해 구성된 WildFire 어플라이언스에 사용자 지정 인증서 적용 518
Panorama Management에서 WildFire 어플라이언스 제거 521
WildFire 클러스터 관리 522
Panorama에서 중앙 집중식으로 클러스터 구성 522
Panorama를 사용하여 WildFire 클러스터 상태 보기 549

라이선스 및 업데이트 관리 551
Panorama를 사용하여 방화벽에서 라이선스 관리 552

네트워크 활동 모니터링 555
가시성을 위해 Panorama 사용 556
ACC 및 AppScope로 네트워크 모니터링 556
로그 데이터 분석 558
보고서 생성, 예약 및 이메일로 보내기 558
예약된 보고서에 대한 주요 제한 구성 562
Panorama의 ESM 로그 수집 트랩 565
사용 사례: Panorama를 사용하여 애플리케이션 모니터링 567
사용 사례: Panorama를 사용하여 사고에 대응 570
사고 알림 570
ACC의 위젯 검토 571
위협 로그 검토 571
WildFire 로그 검토 572

 ©2024 Palo Alto Networks, Inc.

데이터 필터링 로그 검토 572
보안 규칙 업데이트 573

Panorama 고가용성 575

Panorama HA 전제 조건 576
HA의 Panorama에 대한 우선 순위 및 페일오버 578
페일오버 트리거 579
HA 하트비트 폴링 및 Hello 메시지 579
HA 경로 모니터링 579
Panorama HA의 로깅 고려 사항 580
레거시 모드에서 Panorama 가상 어플라이언스의 페일오버 로깅 580
Panorama 모드의 M-시리즈 어플라이언스 또는 Panorama 가상 어플라이언스에서 페일오버 로깅 581
Panorama HA 피어 간의 동기화 582
Panorama HA 쌍 관리 583
Panorama에서 HA 설정 583
HA 피어 간에 사용자 지정 인증서를 사용하여 인증 설정 585
Panorama HA 페일오버 테스트 587
NFS 로깅을 재개하기 위해 Panorama 페일오버 후 우선 순위 전환 587
기본 Panorama를 활성 상태로 복원 588

Panorama 관리 589

구성 변경 사항 미리보기, 검증 또는 커밋 590
관리되는 디바이스에 대한 선택적 구성 변경 커밋 595
선택적 구성 변경 내용을 관리형 디바이스에 푸시 597
자동 커밋 복구 활성화 600
Panorama 및 방화벽 구성 백업 관리 602
구성 파일 내보내기 예약 602
Panorama 및 방화벽 구성 저장 및 내보내기 604
Panorama 구성 변경 사항 되돌리기 606
Panorama에서 최대 구성 백업 수 구성 609
관리되는 방화벽에서 구성 백업 로드 609
구성 감사 수행 610
Panorama 구성의 변경 사항 비교 615
구성 변경 제한을 위한 잠금 관리 616
Panorama에 사용자 정의 로고 추가 618
Panorama 작업 관리자 사용 619
로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 관리 620
로그 및 보고서 저장소 620

 ©2024 Palo Alto Networks, Inc.

로그 및 보고서 만료 기간 621
로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 구성 621
Panorama 보고서의 실행 시간 구성 623
모니터 Panorama 625
Panorama 시스템 및 구성 로그 625
SNMP를 사용하여 Panorama 및 로그 수집기 통계 모니터링 626
Panorama 재부팅 또는 종료 629
Panorama 암호 프로파일 및 복잡성 구성 630

Panorama 플러그인 631

Panorama 플러그인 정보 632
Panorama 플러그인 설치 634
VM 시리즈 플러그인 및 Panorama 플러그인 635
Panorama에 VM 시리즈 플러그인 설치 635
Cisco TrustSec에 대한 엔드포인트 모니터링 637
Cisco TrustSec용 Panorama 플러그인 637
Cisco TrustSec용 Panorama 플러그인 설치 639
Cisco TrustSec용 Panorama 플러그인 구성 640
Cisco TrustSec용 Panorama 플러그인 문제 해결 647

문제 해결 651

Panorama 시스템 문제 해결 652
Panorama에 대한 진단 파일 생성 652
Panorama 정지 상태 진단 652
파일 시스템 무결성 검사 모니터링 652
소프트웨어 및 콘텐츠 업데이트를 위한 Panorama Storage 관리 653
Panorama HA 배포의 스플릿 브레인에서 복구 654
메모리 문제로 인한 Panorama 재부팅 654
로그 저장소 및 연결 문제 해결 656
Panorama 포트 사용 확인 656
수집기 그룹에 대한 Zero Log Storage 해결 658
M-시리즈 어플라이언스에서 장애가 발생한 디스크 교체 659
ESXi 서버에서 가상 디스크 교체 659
vCloud Air에서 가상 디스크 교체 660
로그 수집기 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션 660
Panorama 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션 667
고가용성의 Panorama 모드에서 새로운 M-시리즈 어플라이언스 모델로 로그 마이그레이션 675
고가용성의 Panorama 모드에서 동일한 M 시리즈 어플라이언스 모델로 로그 마이그레이션 684

 ©2024 Palo Alto Networks, Inc.

비HA Panorama의 실패/RMA 후 로그 수집기 마이그레이션 694
M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성 699
로그 쿼리 작업 보기 700
RMA 방화벽 교체 701
방화벽에 대한 부분적 디바이스 상태 생성 701
RMA 방화벽 교체를 시작하기 전 701
교체 후 방화벽 구성 복원 702
커밋 실패 문제 해결 708
Panorama에서 커밋 문제 분류 709
템플릿 또는 디바이스 그룹 푸시 실패 문제 해결 711
보류 중인 로컬 방화벽 변경으로 인한 Panorama 푸시 실패 문제 해결 713
등록 또는 일련번호 오류 문제 해결 714
보고 오류 문제 해결 715
디바이스 관리 라이선스 오류 문제 해결 716
자동으로 되돌린 방화벽 구성 문제 해결 717
작업 성공 또는 실패 상태 보기 719
관리되는 디바이스에 대한 정책 일치 및 연결 테스트 720
정책 규칙 트래픽 일치 문제 해결 720
네트워크 리소스에 대한 연결 문제 해결 721
관리되는 방화벽에 대한 통계 덤프 파일 생성 723
Panorama에 대한 관리 디바이스 연결 복구 725
만료된 디바이스 인증서 복원 728

 ©2024 Palo Alto Networks, Inc.

Panorama 개요

Panorama™ 관리 서버는 여러 Palo Alto Networks 차세대 방화벽과 WildFire 어플라이언스 및 어플라이언스 클러스터에 대한 중앙 집중식 모니터링 및 관리를 제공합니다. 네트워크를 통과하는 모든 애플리케이션, 사용자 및 콘텐츠를 감독할 수 있는 단일 위치를 제공하고 이 지식을 사용하여 네트워크를 보호하고 제어하는 애플리케이션 활성화 정책을 생성합니다. 중앙 집중식 정책 및 방화벽 관리에 Panorama를 사용하면 분산된 방화벽 네트워크를 관리하고 유지하는 데 운영 효율성이 높아집니다. 중앙 집중식 WildFire 어플라이언스 및 WildFire 어플라이언스 클러스터 관리에 Panorama를 사용하면 단일 네트워크가 지원하는 방화벽 수가 증가하고 내결함성을 위한 고가용성이 제공되며 관리 효율성이 높아집니다.

- Panorama 정보
- Panorama 모델
- 중앙 집중식 방화벽 구성 및 업데이트 관리
- 중앙 집중식 로깅 및 보고
- Panorama를 사용한 데이터 재배포
- 역할 기반 액세스 제어
- Panorama 커밋, 검증 및 미리보기 작업
- Panorama 배포 계획
- Panorama 배포: 작업 개요

Panorama 정보

Panorama를 사용하면 중앙 감시를 통해 Palo Alto Networks 방화벽을 효과적으로 구성, 관리 및 모니터링할 수 있습니다. Panorama가 가치를 더하는 세 가지 주요 영역은 다음과 같습니다.

- 중앙 집중식 구성 및 배포 - 네트워크에서 방화벽 및 WildFire 어플라이언스의 중앙 관리 및 신속한 배포를 단순화하려면 Panorama를 사용하여 배포를 위해 방화벽 및 WildFire 어플라이언스를 사전 준비합니다. 그런 다음 방화벽을 그룹으로 조합하고 템플릿을 만들어 기본 네트워크 및 디바이스 구성을 적용하고 디바이스 그룹을 사용하여 전역 공유 및 로컬 정책 규칙을 관리할 수 있습니다. 중앙 집중식 방화벽 구성 및 업데이트 관리를 참조하십시오.
- 분석 및 보고를 위한 중앙 감시 기능이 있는 집계 로깅 - 네트워크의 모든 관리 방화벽에서 활동에 대한 정보를 수집하고 데이터를 중앙에서 분석, 조사 및 보고합니다. 네트워크 트래픽, 사용자 활동 및 관련 위험에 대한 포괄적인 보기를 통해 다양한 정책 세트를 사용하여 잠재적 위협에 대응하고 네트워크에서 애플리케이션을 안전하게 활성화할 수 있습니다. 중앙 집중식 로깅 및 보고를 참조하십시오.
- 분산 관리 - 전역 및 로컬 방화벽 구성 및 정책에 대한 액세스를 위임하거나 제한할 수 있습니다. 분산 관리를 위한 적절한 액세스 수준의 위임은 역할 기반 액세스 제어를 참조하십시오.

Panorama 가상 어플라이언스, M-600 어플라이언스, M-500 어플라이언스, M-200 어플라이언스 등 6가지 Panorama 모델을 사용할 수 있으며, PAN-OS 10.0 이상 릴리스에서 지원됩니다. M-300 어플라이언스 및 M-700 어플라이언스는 PAN-OS 10.2 이상 릴리스에서 지원됩니다.Panorama 중앙 집중식 관리에서는 방화벽을 관리하기 위해 고가용성(HA) 구성으로 Panorama를 배포하는 방법을 설명합니다.

©2024 Palo Alto Networks, Inc.

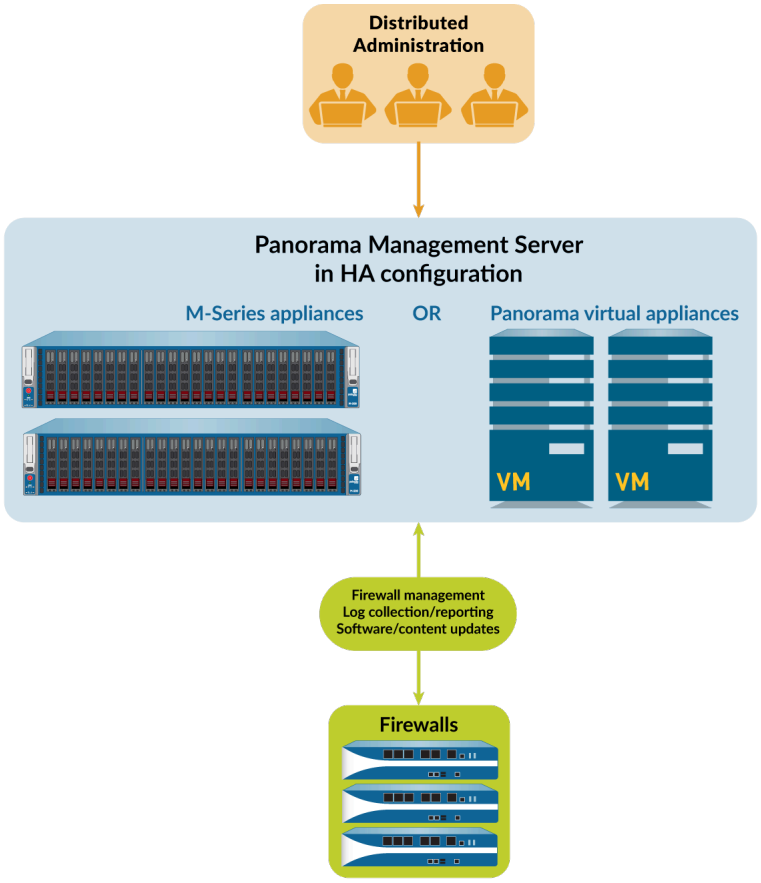


그림 **1: Panorama** 중앙 집중식 관리

©2024 Palo Alto Networks, Inc.

Panorama 모델

Panorama는 다음과 같은 가상 또는 물리적 어플라이언스 중 하나로 사용할 수 있으며 각 어플라이언스는 최대 25, 100 또는 1,000개의 방화벽을 관리하기 위한 라이선스를 지원합니다. 또한 M-600 및 M-700 어플라이언스는 최대 5,000개의 방화벽을 관리하기 위한 라이선스를 지원하고 유사하게 리소스가 할당된 Panorama 가상 어플라이언스는 최대 2,500개의 방화벽을 관리하기 위한 라이선스를 지원합니다.

- **Panorama** 가상 어플라이언스 - 이 모델은 간단한 설치를 제공하고 가상 관리 어플라이언스가 필요한 사이트에 대한 서버 통합을 용이하게 합니다. Alibaba Cloud, Amazon Web Services(AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform(GCP), KVM, Hyper-V, Oracle Cloud Infrastructure(OCI), VMware ESXi 서버 또는 VMware vCloud에 Panorama를 설치할 수 있습니다. 공기. 가상 어플라이언스는 초당 최대 20,000개의 로그 속도로 로컬에서 방화벽 로그를 수집할 수 있으며 더 높은 로깅 속도를 위해 전용 로그 수집기를 관리할 수 있습니다. 가상 어플라이언스는 전용 관리 서버, 로컬 로그 수집 기능이 있는 Panorama 관리 서버 또는 전용 로그 수집기로 기능할 수 있습니다. 지원되는 인터페이스, 로그 저장 용량 및 최대 로그 수집 속도는 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오. 다음 모드에서 가상 어플라이언스를 배포할 수 있습니다.
  - **Panorama** 모드 - 이 모드에서 Panorama 가상 어플라이언스는 1~12개의 가상 로깅 디스크가 있는 로컬 로그 수집기를 지원합니다(로컬 로그 수집기로 Panorama 가상 어플라이언스 배포 참조). 각 로깅 디스크에는 단일 가상 어플라이언스에서 총 최대 24TB, 고가용성(HA) 쌍에서 48TB에 대한 2TB의 스토리지 용량이 있습니다. Panorama 모드에서만 기존 디스크의 로그 손실 없이 여러 가상 로깅 디스크를 추가할 수 있습니다. Panorama 모드는 또한 더 빠른 보고서 생성의 이점을 제공합니다. Panorama 모드에서 가상 어플라이언스는 NFS 스토리지를 지원하지 않습니다.

    가장 좋은 방법은 가상 어플라이언스를 *Panorama* 모드로 배포하여 로그 스토리지 및 보고서 생성을 최적화하는 것입니다.
  - 레거시 모드(ESXi 및 vCloud Air만 해당) - 이 모드에서 Panorama 가상 어플라이언스는 로컬 로그 수집기를 사용하지 않고 방화벽 로그를 수신하고 저장합니다(로컬 로그 수집을 사용하여 레거시 모드에서 Panorama 가상 어플라이언스 배포 참조). 기본적으로 레거시 모드의 가상 어플라이언스에는 모든 데이터에 대해 하나의 디스크 파티션이 있습니다. 약 11GB의 파티션이 로그 스토리지에 할당됩니다. 로컬 로그 스토리지가 더 필요한 경우 ESXi 5.5 이상의 버전 또는 vCloud Air에서 최대 8TB의 가상 디스크 하나를 추가할 수 있습니다. 이전 ESXi 버전은 최대 2TB의 가상 디스크 1개를 지원합니다. 8TB 이상이 필요한 경우 레거시 모드의 가상 디바이스를 NFS 데이터 저장소에 마운트할 수 있지만 vCloud Air가 아닌 ESXi 서버에만 마운트할 수 있습니다. 이 모드는 Panorama 가상 어플라이언스가 PAN-OS 10.0으로 업그레이드할 때 레거시 모드인 경우에만 사용할 수 있습니다. PAN-OS 9.0 이상 버전으로 업그레이드할 때 다른 모드로 변경하면 레거시 모드를 더 이상 사용할 수 없습니다. Panorama 가상 어플라이언스를 레거시 모드에서 사용 가능한 모드 중 하나로 변경하면 더 이상 레거시 모드로 다시 변경할 수 없습니다.

    지원되지만 레거시 모드는 프로덕션 환경에 권장되지 않지만 랩 또는 데모 환경에서는 계속 사용할 수 있습니다.
  - 관리 전용 모드 - 이 모드에서 Panorama 가상 어플라이언스는 관리되는 디바이스 및 전용 로그 수집기를 위한 전용 관리 어플라이언스입니다. 또한 적절하게 리소스가 할당된 Panorama 가상 어플라이언스는 이 모드에서 최대 2,500개의 방화벽을 관리할 수 있습니다. Panorama 가상 어플라이언스에는 구성 및 시스템 로그를 제외하고는 로그 수집 기능이 없으며 이러한 저장 로그에 대한 전용 로그 수집기가 필요합니다. 기본적으로 관리 전용 모드의 가상 어플라이언스에는 모든 데이터에

 ©2024 Palo Alto Networks, Inc.

대해 하나의 디스크 파티션만 있으므로 관리 전용 모드의 Panorama 가상 어플라이언스로 포워딩된 모든 로그는 삭제됩니다. 따라서 관리 대상 어플라이언스의 로그 데이터를 저장하려면 관리 대상 디바이스의 로그 데이터를 저장하기 위해 로그 포워딩을 구성해야 합니다. 자세한 내용은 디바이스 관리 용량 요구 사항 증가를 참조하십시오.

- 로그 수집기 모드 - Panorama 가상 어플라이언스는 전용 로그 수집기로 작동합니다. 여러 방화벽이 대량의 로그 데이터를 포워딩하는 경우 로그 수집기 모드의 Panorama 가상 어플라이언스는 향상된 확장성과 성능을 제공합니다. 이 모드에서 어플라이언스에는 관리 액세스를 위한 웹 인터페이스가 없습니다. 명령줄 인터페이스(CLI)만 있습니다. 그러나 Panorama 관리 서버의 웹 인터페이스를 사용하여 어플라이언스를 관리할 수 있습니다. Log Collector 모드에서 Panorama 가상 어플라이언스에 대한 CLI 액세스는 초기 설정 및 디버깅에만 필요합니다. 구성 세부 정보는 전용 로그 수집기로 Panorama 배포를 참조하십시오.

- **M** 시리즈 어플라이언스 - M-200, M-300, M-500, M-600 및 M-700 어플라이언스는 대규모 배포를 위한 전용 하드웨어 어플라이언스입니다. 높은 로깅 속도(초당 10,000개 이상의 로그) 및 로그 보존 요구 사항이 있는 환경에서 이러한 어플라이언스를 사용하면 로그 수집 인프라를 확장할 수 있습니다. 지원되는 인터페이스, 로그 저장 용량 및 최대 로그 수집 속도는 M-시리즈 어플라이언스 인터페이스을(를) 참조하십시오. 모든 M-시리즈 모델은 다음 속성을 공유합니다.
  - 방화벽 로그를 저장하는 RAID 드라이브 및 디스크 오류로부터 보호하기 위한 RAID 1 미러링
  - Panorama 및 Log Collectors가 생성하는 로그를 저장하는 SSD
  - 1Gbps 처리량을 지원하는 MGT, Eth1, Eth2 및 Eth3 인터페이스
  - 이중화, 핫스왑 가능한 전원 공급 디바이스
  - 앞뒤 에어플로우

  M-500 및 M-600 어플라이언스에는 다음과 같은 추가 속성이 있어 데이터 센터에 더 적합합니다.

  - 10Gbps 처리량을 지원하는 Eth4 및 Eth5 인터페이스

  또한 다음 속성은 M-600 및 M-700 어플라이언스를 대규모 방화벽 배포에 더 적합하게 생성합니다.

  - 관리 전용 모드의 M-600 및 M-700 어플라이언스는 최대 5,000개의 방화벽을 관리할 수 있습니다.

  다음 모드에서 M-시리즈 어플라이언스를 배포할 수 있습니다.

  - **Panorama** 모드 - 어플라이언스는 방화벽 및 전용 로그 수집기를 관리하는 Panorama 관리 서버로 작동합니다. 어플라이언스는 또한 방화벽 로그를 집계하는 로컬 로그 수집기를 지원합니다. Panorama 모드는 기본 모드입니다. 구성에 대한 자세한 내용은 로컬 로그 수집기를 사용하여 Panorama M-시리즈 어플라이언스 배포를 참조하십시오.
  - 관리 전용 모드 - Panorama 어플라이언스는 관리 디바이스 및 전용 로그 수집기를 위한 전용 관리 어플라이언스입니다. Panorama 어플라이언스에는 구성 및 시스템 로그를 제외하고는 로그 수집 기능이 없으며 배포에는 이러한 로그를 저장하기 위한 전용 로그 수집기가 필요합니다. 기본적으로 관리 전용 모드의 Panorama 어플라이언스에는 모든 데이터에 대해 하나의 디스크 파티션만 있으므로 관리 전용 모드의 Panorama 가상 어플라이언스로 포워딩된 모든 로그는 삭제됩니다. 따라서 관리 대상 어플라이언스의 로그 데이터를 저장하려면 관리 대상 디바이스의 로그 데이터를 저장하기 위해 로그 포워딩을 구성해야 합니다.
  - 로그 수집기 모드 - 어플라이언스는 전용 로그 수집기로 작동합니다. 여러 방화벽이 대량의 로그 데이터를 포워딩하는 경우 로그 수집기 모드의 M-시리즈 어플라이언스는 향상된 확장성과 성능을 제공합니다. 이 모드에서 어플라이언스에는 관리 액세스를 위한 웹 인터페이스가 없습니다. 명령줄 인터페이스(CLI)만 있습니다. 그러나 Panorama 관리 서버의 웹 인터페이스를 사용하여 어플라이언스

©2024 Palo Alto Networks, Inc.

를 관리할 수 있습니다. Log Collector 모드에서 M-시리즈 어플라이언스에 대한 CLI 액세스는 초기 설정 및 디버깅에만 필요합니다. 구성 세부 정보는 전용 로그 수집기로 Panorama 배포를 참조하십시오.

M-시리즈 어플라이언스에 대한 자세한 내용 및 사양은 M-시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

중앙 집중식 방화벽 구성 및 업데이트 관리

Panorama™는 디바이스 그룹과 템플릿을 사용하여 방화벽을 유사한 구성이 필요한 논리적 세트로 그룹화합니다. 디바이스 그룹 및 템플릿을 사용하여 관리되는 방화벽의 모든 구성 요소, 정책 및 개체를 중앙에서 관리합니다. Panorama를 사용하면 라이선스, 소프트웨어(PAN-OS® 소프트웨어, SSL-VPN 클라이언트 소프트웨어, GlobalProtect™ 에이전트/앱 소프트웨어) 및 콘텐츠 업데이트(애플리케이션, 위협, WildFire® 및 바이러스 백신)를 중앙에서 관리할 수도 있습니다. 모든 디바이스 그룹, 템플릿 및 템플릿 스택 구성 개체는 이름이 고유해야 합니다.

관리되는 방화벽 또는 Panorama가 예기치 않게 다시 시작되는 경우 디바이스 그룹 및 템플릿의 커밋되지 않은 모든 구성 변경 사항은 변경 사항을 성공적으로 커밋할 때까지 로컬로 보존됩니다. 재시작은 방화벽이나 Panorama 또는 구성 관리와 관련된 PAN-OS 관리 프로세스의 재시작일 수 있습니다. 고가용성(HA) 구성의 방화벽 또는 Panorama의 경우 예기치 않은 다시 시작 시 커밋되지 않은 구성 변경 사항이 HA 피어 간에 자동으로 동기화되지 않습니다.

- 컨텍스트 스위치 - 방화벽 또는 Panorama
- Panorama의 총 구성 크기
- 템플릿 및 템플릿 스택(template stack)
- 디바이스 그룹

컨텍스트 스위치 - 방화벽 또는 Panorama

Panorama™ 웹 인터페이스를 사용하면 모든 탭의 왼쪽 상단에 있는 컨텍스트 드롭다운을 사용하여 Panorama 중심 보기와 방화벽 중심 보기 간에 전환할 수 있습니다. 컨텍스트를 **Panorama**로 설정하여 방화벽을 중앙에서 관리하거나 컨텍스트를 특정 방화벽의 웹 인터페이스로 전환하여 로컬로 구성합니다. Panorama와 방화벽 웹 인터페이스의 유사성은 방화벽을 모니터링하고 관리하기 위해 원활하게 둘 사이를 이동할 수 있도록 합니다.

컨텍스트 드롭다운에는 Panorama에 연결된 방화벽만 나열됩니다. 디바이스 그룹 및 템플릿 관리자의 경우 드롭다운에는 해당 관리자에게 할당된 액세스 도메인 내에 있는 연결된 방화벽만 나열됩니다. 긴 목록을 검색하려면 드롭다운 내의 필터를 사용하십시오.

고가용성(HA) 구성의 방화벽의 경우 아이콘에는 HA 상태를 나타내는 색상 배경이 있습니다(다음과 같이). HA 상태를 아는 것은 방화벽 컨텍스트를 선택할 때 유용합니다. 예를 들어 일반적으로 활성 방화벽에서 방화벽별 구성을 변경합니다.

- 녹색 - 활성.
- 노란색 - 수동 또는 방화벽이 시작 중입니다(시작 상태는 부팅 후 최대 60초 동안 지속됨).
- 빨간색 - 방화벽이 작동 중단(오류 상태), 일시 중단(관리자가 방화벽을 비활성화함) 또는 임시(활성/활성 HA 구성에서 링크 또는 경로 모니터링 이벤트의 경우) 상태입니다.

디바이스 그룹 및 템플릿 관리자에 대한 관리자 역할 프로파일을 구성할 때 관리 방화벽에 푸시되는 디바이스 관리자 역할을 Panorama와 방화벽 웹 인터페이스 간의 컨텍스트 전환에 할당해야 합니다.

컨텍스트 전환 중에 Panorama는 관리자에게 특정 vsys 또는 모든 vsys에 대한 액세스 권한이 있는지 확인합니다. 관리자가 모든 vsys에 액세스할 수 있는 경우 Panorama는 디바이스 관리자 역할 컨텍스트 스위치를 사용합니다. 관리자가 vsys 중 하나 또는 일부에 액세스할 수 있는 경우 Panorama는 vsys 관리자 역할을 사용하여 컨텍스트 전환을 수행합니다.

©2024 Palo Alto Networks, Inc.

Panorama의 총 구성 크기

Panorama™ M-시리즈 및 가상 어플라이언스의 총 구성 파일 크기는 성능 메트릭의 중요한 부분으로, 어떤 M-시리즈 어플라이언스 또는 Panorama 가상 어플라이언스에 할당해야 하는 가상 리소스의 최소량을 귀하의 보안 요구 사항. Panorama 관리 서버의 지원되는 총 구성 파일 크기를 초과하면 구성 변경, 커밋 및 관리 방화벽에 대한 푸시를 수행할 때 성능이 저하됩니다.

Panorama 모드의 Panorama 관리 서버는 모든 템플릿, 디바이스 그룹 및 Panorama 특정 구성에 대해 80MB의 총 구성 파일 크기를 지원합니다. Panorama가 관리 전용 모드에서 지원하는 최대 구성 파일 크기는 Panorama 모델이나 Panorama 가상 어플라이언스에 할당한 리소스에 따라 달라집니다. Panorama M-Series 어플라이언스 모델 또는 Panorama 가상 어플라이언스에 할당한 리소스에 따라 권장되는 최대 구성 파일 크기는 아래 표를 참조하십시오.

Panorama 모델	필요한 가상 리소스	관리 전용 모드의 최대 구성 파일 크기	**Panorama** 모드의 최대 구성 파일 크기
M-200	해당 사항 없음	120MB	80MB
M-300		150MB	
M-500		120MB	
M-600		150MB	
M-700		180MB	
Panorama 가상 어플라이언스 추가 설정 정보는 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.	• 16개의 vCPU • 128GB 메모리	120MB	
	• 56개의 vCPU • 256GB 메모리	150MB	

템플릿 및 템플릿 스택(template stack)

템플릿 및 템플릿 스택(template stack)을 사용하여 방화벽이 네트워크에서 작동할 수 있도록 하는 설정을 구성합니다. 템플릿은 Panorama™에서 네트워크 및 디바이스 탭을 구성하는 데 사용하는 기본 빌딩 블록입니다. 템플릿을 사용하여 인터페이스 및 영역 구성을 정의하고, 로깅 및 syslog 액세스를 위한 서버 프로파일을 관리하거나, VPN 구성을 정의할 수 있습니다. 템플릿 스택(template stack)을 사용하면 여러 템플릿을 계층화하고 결합된 구성을 생성할 수 있습니다. 템플릿 스택(template stack)을 사용하면 템플릿 스택(template stack)에 연결된 모든 디바이스에 대한 공통 기본 구성을 정의할 수 있고 템플릿을 계층화하여 결합된 구성을 생성할 수 있기 때문에 관리를 단순화합니다. 이를 통해 위치 또는 기능별 설정으로 템플릿을 정의한 다음 방화벽이 스택의 템플릿 순서를 기반으로 설정을 상속하도록 우선 순위의 내림차순에 따라 템플릿을 스택할 수 있습니다.

©2024 Palo Alto Networks, Inc.

템플릿과 템플릿 스택(template stack) 모두 변수를 지원합니다. 변수를 사용하면 구성 요구 사항에 따라 템플릿 또는 템플릿 스택(template stack)에 지정된 값으로 자리 표시자 개체를 생성할 수 있습니다. 구성에서 IP 주소, 그룹 ID 및 인터페이스를 대체할 템플릿 또는 템플릿 스택(template stack) 변수를 생성합니다. 템플릿 변수는 템플릿 스택(template stack)에 상속되며 템플릿 스택(template stack) 변수를 생성하기 위해 재정의할 수 있습니다. 그러나 템플릿은 템플릿 스택(template stack)에 정의된 변수를 상속하지 않습니다. 템플릿 또는 템플릿 스택(template stack)에 변수가 정의되어 방화벽에 푸시되면 변수에 대해 정의된 값이 방화벽에 표시됩니다.

템플릿을 사용하여 고유한 설정이 있는 방화벽을 수용합니다. 또는 더 광범위한 공통 기본 구성을 푸시한 다음 푸시된 특정 설정을 개별 방화벽의 방화벽별 값으로 재정의할 수 있습니다. 방화벽의 설정을 무시하면 방화벽은 해당 설정을 로컬 구성에 저장하고 Panorama는 더 이상 설정을 관리하지 않습니다. 템플릿 값을 재정의한 후 복원하려면 Panorama를 사용하여 템플릿 또는 템플릿 스택(template stack) 구성을 방화벽에 적용합니다. 예를 들어 템플릿에서 공통 NTP 서버를 정의하고 방화벽의 NTP 서버 구성을 재정의하여 현지 표준 시간대를 수용한 후 추후에 템플릿에 정의된 NTP 서버로 되돌릴 수 있습니다.

템플릿 스택(template stack)을 정의할 때 동일한 하드웨어 모델이고 게이트웨이 및 syslog 서버와 같은 유사한 네트워크 리소스에 대한 액세스가 필요한 방화벽을 할당하는 것을 고려하십시오. 이렇게 하면 모든 템플릿 스택(template stack)에 모든 설정을 추가하는 중복을 피할 수 있습니다. 다음 그림은 아시아 태평양(APAC) 지역의 데이터 센터 방화벽을 전역 설정이 있는 스택, APAC별 설정이 있는 하나의 템플릿, 데이터 센터별 설정이 있는 하나의 템플릿에 할당하는 구성의 예를 보여줍니다. APAC 지사에서 방화벽을 관리하려면 지사별 설정이 있는 템플릿이 포함된 다른 스택에 글로벌 및 APAC별 템플릿을 추가하여 재사용할 수 있습니다. 스택의 템플릿에는 Panorama가 중복 설정에 대해 하나의 값만 푸시하도록 구성 가능한 우선순위가 있습니다. Panorama는 스택 구성에 나열된 템플릿을 우선 순위가 높은 템플릿을 사용하여 위에서 아래로 평가합니다. 다음 그림은 데이터 센터 템플릿이 글로벌 템플릿보다 우선 순위가 높은 데이터 센터 스택을 보여줍니다. Panorama는 데이터 센터 템플릿에서 유휴 타임아웃 값을 푸시하고 전역 템플릿의 값을 무시합니다.

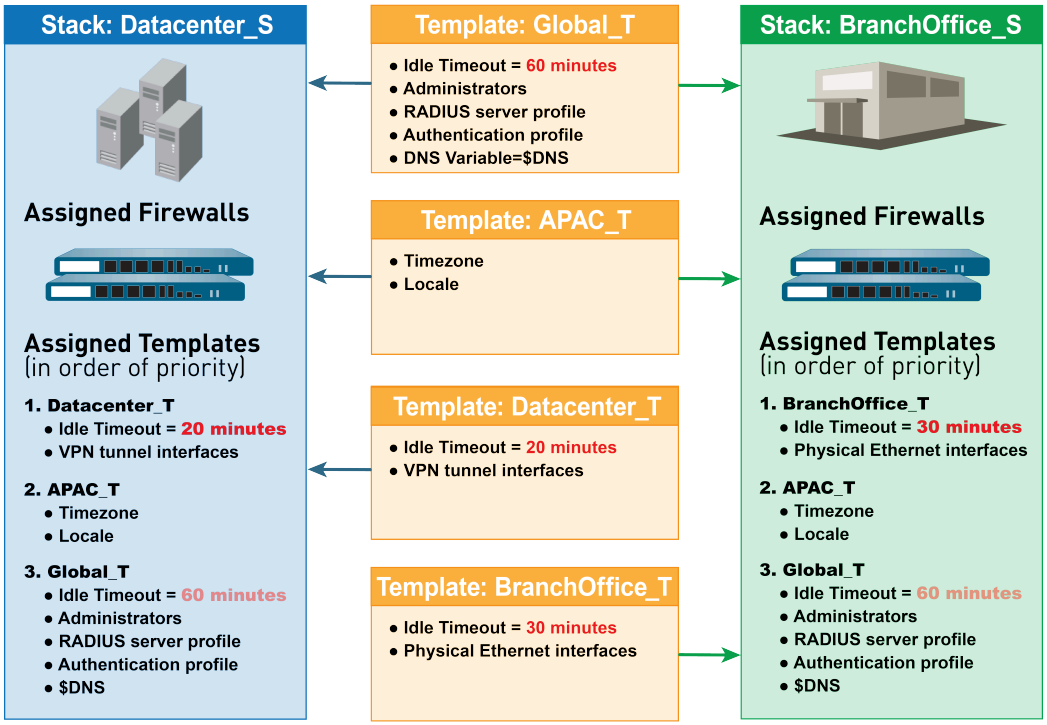


그림 **2:** 템플릿 스택**(template stack)**

 ©2024 Palo Alto Networks, Inc.

템플릿 또는 템플릿 스택(template stack)을 사용하여 VPN(가상 사설망) 모드, 다중 가상 시스템(multi-vsys) 모드 또는 작동 모드(일반 또는 FIPS-CC 모드)와 같은 방화벽 모드를 설정할 수 없습니다. 자세한 내용은 템플릿 기능 및 예외를 참조하십시오. 그러나 일치하지 않는 모드가 있는 방화벽을 동일한 템플릿 또는 스택에 할당할 수 있습니다. 이러한 경우 Panorama는 모드별 설정을 해당 모드를 지원하는 방화벽에만 푸시합니다. 예외적으로 가상 시스템을 지원하지 않거나 구성된 가상 시스템이 없는 방화벽에 템플릿의 기본 vsys 설정을 푸시하도록 Panorama를 구성할 수 있습니다.

관련 절차는 템플릿 및 템플릿 스택(template stack) 관리를 참조하십시오.

디바이스 그룹

Panorama를 효과적으로 사용하려면 네트워크의 방화벽을 디바이스 그룹이라는 논리적 단위로 그룹화해야 합니다. 디바이스 그룹을 사용하면 네트워크 세분화, 지리적 위치, 조직 기능 또는 유사한 정책 구성이 필요한 방화벽의 기타 일반적인 측면을 기반으로 그룹화할 수 있습니다. 디바이스 그룹을 사용하여 정책 규칙과 정책 규칙이 참조하는 개체를 구성할 수 있습니다. 공유 규칙 및 개체가 맨 위에 있고 디바이스 그룹별 규칙 및 개체가 후속 수준에 있는 상태에서 디바이스 그룹을 계층적으로 구성할 수 있습니다. 이를 통해 방화벽이 트래픽을 처리하는 방법을 적용하는 규칙 계층을 만들 수 있습니다. 예를 들어 공유 규칙 집합을 회사의 사용 제한 정책으로 정의할 수 있습니다. 그런 다음 지역 사무소만 BitTorrent와 같은 P2P 트래픽에 액세스할 수 있도록 Panorama가 지역 사무소에만 푸시하는 디바이스 그룹 규칙을 정의할 수 있습니다(또는 공유 보안 규칙을 정의하고 지역 사무소를 대상으로 함). 관련 절차는 디바이스 그룹 관리을(를) 참조하십시오. 다음 항목에서는 디바이스 그룹 개념 및 구성 요소에 대해 자세히 설명합니다.

- 디바이스 그룹 계층
- 디바이스 그룹 정책
- 디바이스 그룹 개체

디바이스 그룹 계층

디바이스 그룹 계층 생성을(를) 수행하면 상위 수준 그룹의 설정(정책 규칙 및 개체)을 상속하는 하위 수준 그룹과 함께 최대 4개 수준의 트리 계층 구조에서 디바이스 그룹을 중첩할 수 있습니다. 최하위 계층에서 디바이스 그룹에는 상위, 조부모 및 증조부모 디바이스 그룹(상위)이 있을 수 있습니다. 최상위 계층에서 디바이스 그룹에는 자식, 손자 및 증손자 디바이스 그룹(하위 항목)이 있을 수 있습니다. 공유 위치에서 설정을 상속하는 모든 디바이스 그룹(모든 디바이스 그룹의 공통적인 구성에 대한 계층 구조의 맨 위에 있는 컨테이너).

디바이스 그룹 계층을 생성하면 중복 구성 없이 공통 정책 요구 사항에 따라 방화벽을 구성할 수 있습니다. 예를 들어, 모든 방화벽에 전역적으로 적용되는 공유 설정을 구성하고, 첫 번째 수준에서 기능별 설정으로 디바이스 그룹을 구성하고, 더 낮은 수준에서 위치별 설정으로 디바이스 그룹을 구성할 수 있습니다. 계층 구조가 없으면 공유 아래의 단일 수준에서 모든 디바이스 그룹에 대한 기능 및 위치별 설정을 모두 구성해야 합니다.

 ©2024 Palo Alto Networks, Inc.

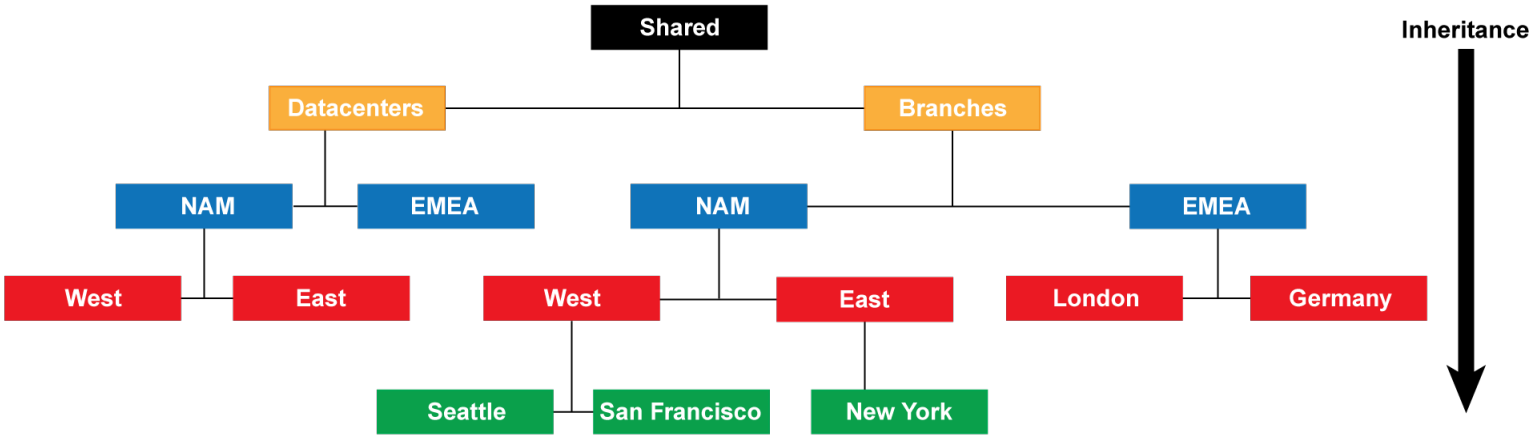
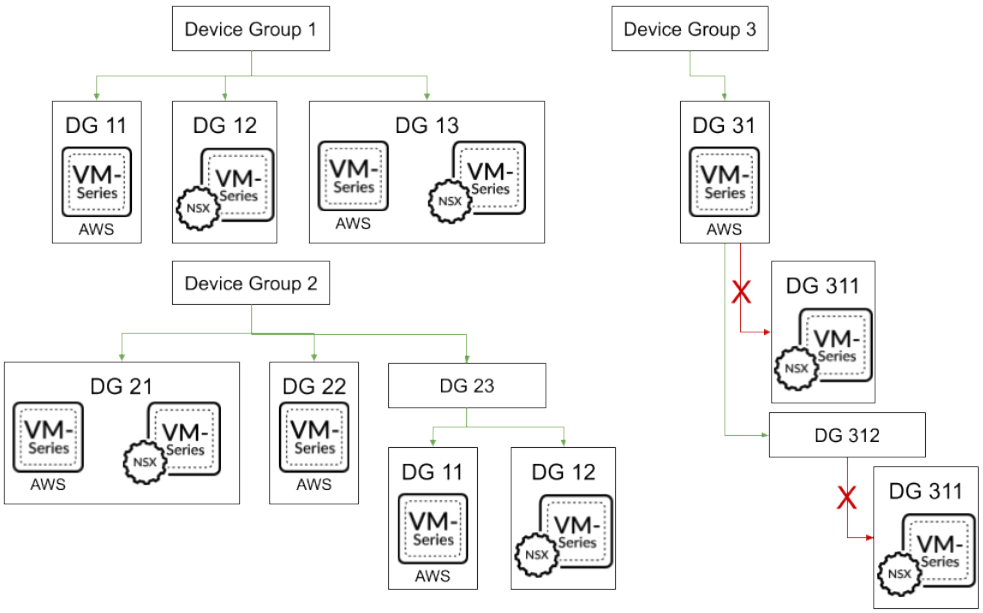


그림 **3:** 디바이스 그룹 계층

방화벽이 디바이스 그룹 계층에서 정책 규칙을 평가하는 순서에 대한 자세한 내용은 디바이스 그룹 정책을(를) 참조하십시오. 디바이스 그룹이 상위 디바이스 그룹에서 상속하는 개체의 값 재정의에 대한 자세한 내용은 디바이스 그룹 개체을(를) 참조하십시오.

수행할 다중 Panorama 플러그인 배포에서 특정 하이퍼바이저에 배포된 방화벽이 포함된 디바이스 그룹은 다른 하이퍼바이저에 배포된 방화벽이 포함된 디바이스 그룹의 하위 또는 상위가 될 수 없습니다. 예를 들어 Panorama가 VMware NSX-V 및 AWS로부터 IP 주소 업데이트를 수신하는 경우 AWS VM-시리즈 방화벽 디바이스 그룹의 하위인 NSX-V VM-시리즈 방화벽의 디바이스 그룹을 생성할 수 없습니다.



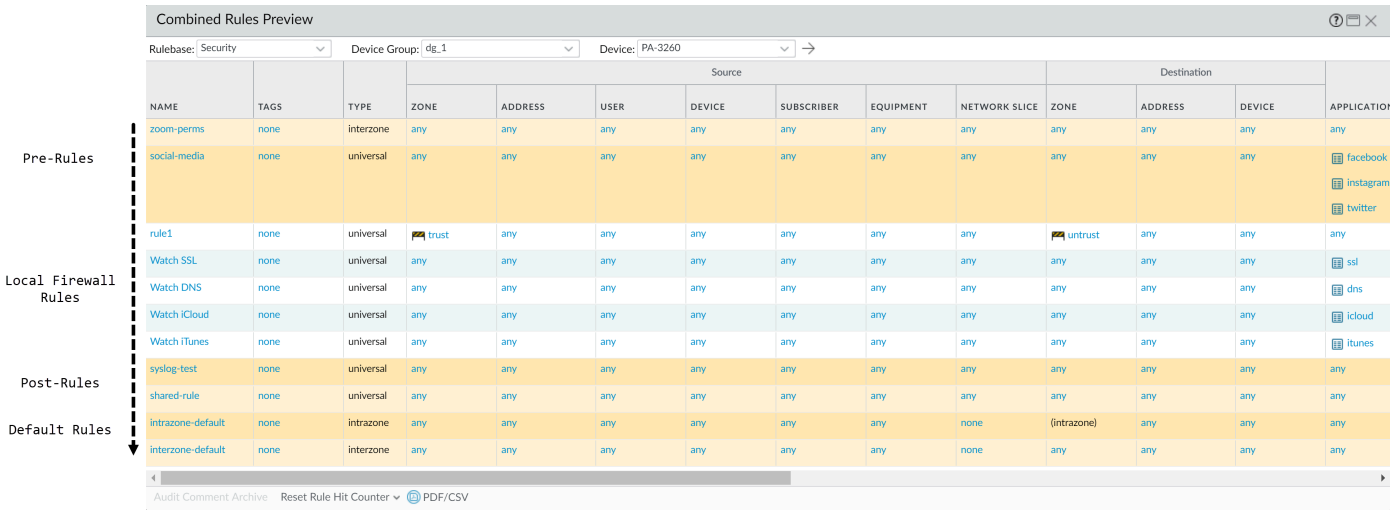
디바이스 그룹 정책

디바이스 그룹은 관리되는 방화벽 네트워크에서 정책을 관리하기 위한 계층화된 접근 방식을 구현하는 방법을 제공합니다. 방화벽은 계층(공유, 디바이스 그룹 및 로컬) 및 유형(사전 규칙, 사후 규칙 및 기본 규칙)별로 정책 규칙을 위에서 아래로 다음 순서로 평가합니다. 방화벽은 트래픽을 수신할 때 트래픽과 일치하는 첫 번째 평가된 규칙에 정의된 작업을 수행하고 모든 후속 규칙을 무시합니다. 특정 레이어, 유형 및

©2024 Palo Alto Networks, Inc.

규칙 베이스(예: 공유 보안 사전 규칙) 내의 규칙에 대한 평가 순서를 변경하려면 규칙 계층 구조 관리를 참조하십시오.

방화벽에서 규칙을 확인하든 Panorama에서 확인하든 웹 인터페이스는 규칙을 평가 순서로 표시합니다. 방화벽이 Panorama에서 상속하는 모든 공유, 디바이스 그룹 및 기본 규칙은 주황색으로 음영 처리됩니다. 로컬 방화벽 규칙은 사전 규칙과 사후 규칙 사이에 표시됩니다.



평가 순서	규칙 범위 및 설명	관리 디바이스
공유 사전 규칙	Panorama는 공유 사전 규칙을 모든 디바이스 그룹의 모든 방화벽에 푸시합니다. Panorama는 특정 디바이스 그룹 및 해당 하위 디바이스 그룹의 모든 방화벽에 디바이스 그룹별 사전 규칙을 푸시합니다. 방화벽이 디바이스 그룹 계층의 여러 수준에 있는 디바이스 그룹의 규칙을 상속하는 경우 가장 높은 수준에서 가장 낮은 수준의 순서로 사전 규칙을 평가합니다. 즉, 방화벽은 먼저 공유 규칙을 평가하고 하위 항목이 없는 디바이스 그룹의 규칙을 마지막으로 평가합니다. 사전 규칙을 사용하여 조직의 허용 가능한 사용 정책을 시행할 수 있습니다. 예를 들어 사전 규칙은 특정 URL 카테고리에 대한 액세스를 차단하거나 모든 사용자에 대해 DNS(Domain Name System) 트래픽을 허용할 수 있습니다.	이러한 규칙은 방화벽에서 볼 수 있지만 Panorama에서만 관리할 수 있습니다.
디바이스 그룹 사전 규칙		

©2024 Palo Alto Networks, Inc.

평가 순서	규칙 범위 및 설명	관리 디바이스
로컬 방화벽 규칙	로컬 규칙은 단일 방화벽 또는 가상 시스템(vsys)에만 적용됩니다.	로컬 방화벽 관리자 또는 로컬 방화벽 컨텍스트로 전환하는 Panorama 관리자는 로컬 방화벽 규칙을 편집할 수 있습니다.
디바이스 그룹 사후 규칙 공유 사후 규칙	Panorama는 공유 사후 규칙을 모든 디바이스 그룹의 모든 방화벽에 푸시합니다. Panorama는 특정 디바이스 그룹 및 해당 하위 디바이스 그룹의 모든 방화벽에 디바이스 그룹별 사후 규칙을 푸시합니다. 방화벽이 디바이스 그룹 계층 구조의 여러 수준에 있는 디바이스 그룹에서 규칙을 상속하는 경우 가장 낮은 수준에서 가장 높은 수준의 순서로 사후 규칙을 평가합니다. 즉, 방화벽은 하위 항목이 없는 디바이스 그룹의 규칙을 먼저 평가하고 공유 규칙을 마지막으로 평가합니다. 사후 규칙에는 일반적으로 App-ID™ 서명, User-ID™ 정보(사용자 또는 사용자 그룹) 또는 서비스를 기반으로 트래픽에 대한 액세스를 거부하는 규칙이 포함됩니다.	이러한 규칙은 방화벽에서 볼 수 있지만 Panorama에서만 관리할 수 있습니다.
intrazone-default interzone-default	기본 규칙은 보안 규칙 베이스에만 적용되며 Panorama(공유 수준) 및 방화벽(각 vsys)에 사전 정의됩니다. 이 규칙은 PAN-OS가 다른 규칙과 일치하지 않는 트래픽을 처리하는 방법을 지정합니다. intrazone-default 규칙은 영역 내의 모든 트래픽을 허용합니다. interzone-default 규칙은 영역 간의 모든 트래픽을 거부합니다. 기본 규칙을 재정의하면 우선 순위가 가장 낮은 컨텍스트에서 가장 높은 순서로 실행됩니다. 방화벽 수준에서 재정의된 설정은 디바이스 그룹 수준의 설정보다 우선하고 공유 수준의 설정보다 우선합니다.	기본 규칙은 사전 정의된 구성의 일부이거나 Panorama가 해당 규칙을 방화벽으로 푸시했기 때문에 처음에는 읽기 전용입니다. 그러나 태그, 작업, 로깅 및 보안 프로파일에 대한 규칙 설정을 재정의할 수 있습니다. 컨텍스트는 규칙을 재정의할 수 있는 수준을 결정합니다. • Panorama - 공유 또는 디바이스 그룹 수준에서 사전 정의된 구성의 일부인 기본 규칙을 재정의할 수 있습니다. • 방화벽 - 방화벽 또는 vsys에서 사전 정의된 구성의 일부이거나 Panorama가 공유 위치 또는 디바이스 그룹에서 푸시한 기본 규칙을 재정의할 수 있습니다.

©2024 Palo Alto Networks, Inc.

디바이스 그룹 개체

개체는 정책 규칙이 참조하는 구성 요소입니다. 예를 들면 다음과 같습니다. IP 주소, URL 카테고리, 보안 프로파일, 사용자, 서비스 및 애플리케이션. 모든 유형의 규칙(사전 규칙, 사후 규칙, 기본 규칙 및 방화벽에 로컬로 정의된 규칙) 및 모든 규칙 베이스(보안, NAT, QoS, 정책 기반 포워딩, 복호화, 애플리케이션 재정의, 종속 포털 및 DoS 보호) 개체를 참조할 수 있습니다. 디바이스 그룹 계층에서 해당 개체와 범위가 동일한 여러 규칙에서 개체를 재사용할 수 있습니다. 예를 들어 공유 위치에 개체를 추가하면 모든 디바이스 그룹이 공유 상태에서 개체를 상속하므로 계층의 모든 규칙이 해당 공유 개체를 참조할 수 있습니다. 특정 디바이스 그룹에 개체를 추가하는 경우 해당 디바이스 그룹 및 해당 하위 디바이스 그룹의 규칙만 해당 디바이스 그룹 개체를 참조할 수 있습니다. 디바이스 그룹의 개체 값이 상위 디바이스 그룹에서 상속된 값과 달라야 하는 경우 상속된 개체 값을 재정의할 수 있습니다(상속된 개체 값 재정의 단계 참조). 또한 언제든지 상속된 개체 값으로 되돌릴 수 있습니다. 공유 또는 디바이스 그룹 정책에서 사용할 개체를 한 번 생성하고 여러 번 사용하면 관리 오버헤드가 줄어들고 방화벽 정책 전체에서 일관성이 보장됩니다.

Panorama가 시스템 전체에서 개체를 처리하는 방법을 구성할 수 있습니다.

- 사용하지 않는 개체 푸시 - 기본적으로 Panorama는 공유 또는 디바이스 그룹 정책 규칙이 개체를 참조하는지의 여부에 관계없이 모든 개체를 방화벽으로 푸시합니다. 선택적으로 참조된 개체만 푸시하도록 Panorama를 구성할 수 있습니다. 자세한 내용은 사용하지 않는 공유 객체 관리를 참조하십시오.
- 상위 및 하위 개체의 우선 순위 - 기본적으로 계층의 여러 수준에 있는 디바이스 그룹에 이름은 같지만 값이 다른 개체가 있는 경우(예: 재정의로 인해) 하위 디바이스 그룹의 정책 규칙은 개체 값을 사용합니다. 상위 디바이스 그룹 또는 공유 그룹에서 상속된 개체 값 대신 해당 하위 항목에 있습니다. 선택적으로 이 우선 순위를 반대로 하여 Shared 또는 객체를 포함하는 가장 높은 상위 항목의 값을 모든 하위 디바이스 그룹으로 푸시할 수 있습니다. 자세한 내용은 상속된 개체의 우선 순위 관리를 참조하십시오.

©2024 Palo Alto Networks, Inc.

중앙 집중식 로깅 및 보고

Panorama는 관리되는 모든 방화벽의 로그를 집계하고 네트워크의 모든 트래픽에 대한 가시성을 제공합니다. 또한 관리 방화벽에 대한 모든 정책 수정 및 구성 변경에 대한 감사 추적을 제공합니다. Panorama는 로그를 집계하는 것 외에도 SNMP 트랩, 이메일 알림, syslog 메시지 및 HTTP 페이로드로 외부 서버에 포워딩할 수 있습니다.

중앙 집중식 로깅 및 보고를 위해 Panorama와 원활하게 작동하도록 설계된 클라우드 기반 Strata Logging Service를 사용할 수도 있습니다. Strata Logging Service를 사용하면 관리형 방화벽이 Panorama 또는 관리형 로그 수집기 대신 Strata Logging Service 인프라로 로그를 포워딩할 수 있으므로 직접 시간과 노력을 투자하지 않고도 기존 분산 로그 수집 설정을 보강하거나 현재 로깅 인프라를 확장할 수 있습니다.

Panorama의 ACC(Application Command Center)는 모든 방화벽에 대한 통합 보고를 위한 단일 창을 제공합니다. 이를 통해 네트워크 활동을 중앙에서 모니터링하고 트래픽 및 보안 사고를 분석, 조사 및 보고할 수 있습니다. Panorama에서는 Strata Logging Service, Panorama 또는 관리형 로그 수집기(구성된 경우)로 포워딩된 로그에서 로그를 본 후 보고서를 생성하거나 관리형 방화벽을 직접 쿼리할 수 있습니다. 예를 들어 Panorama(및 관리형 수집기)에 저장된 로그를 기반으로 관리형 방화벽 또는 Strata Logging Service에 로컬로 저장된 로그에 액세스하여 관리형 네트워크의 트래픽, 위협 및/또는 사용자 활동에 대한 보고서를 생성할 수 있습니다.

Strata Logging Service 또는 Panorama에 대한 로그 포워딩을 구성하지 않은 경우 각 관리형 방화벽에서 실행되도록 보고서를 예약하고 결과를 Panorama에 포워딩하여 사용자 활동 및 네트워크 트래픽을 함께 볼 수 있습니다. 보고서는 특정 정보 및 활동에 대한 세부적인 드릴다운을 제공하지 않지만 여전히 통합 모니터링 접근 방식을 제공합니다.

- 관리형 수집기 및 수집기 그룹
- 로컬 및 분산 로그 수집
- 여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항
- 로그 포워딩 옵션
- 중앙 집중식 보고

관리형 수집기 및 수집기 그룹

Panorama는 로그 수집기를 사용하여 관리되는 방화벽에서 로그를 집계합니다. 보고서를 생성할 때 Panorama는 로그 정보에 대해 로그 수집기를 쿼리하여 방화벽이 모니터링하는 모든 네트워크 활동에 대한 가시성을 제공합니다. Panorama를 사용하여 로그 수집기를 구성하고 관리하기 때문에 관리 수집기라고도 합니다. Panorama는 두 가지 유형의 로그 수집기를 관리할 수 있습니다.

- 로컬 로그 수집기 - 이 유형의 로그 수집기는 Panorama 관리 서버에서 로컬로 실행됩니다. Panorama 모드의 M-700, M-600, M-500, M-300 또는 M-100 어플라이언스 또는 Panorama 가상 어플라이언스만 로컬 로그 수집기를 지원합니다.

  레거시 모드에서 *Panorama* 가상 어플라이언스에 로그를 포워딩하는 경우 로그 수집기 없이 로컬로 로그를 저장합니다.
- 전용 로그 수집기 - 로그 수집기 모드의 M-700, M-600, M-500, M-300, M-200 또는 M-100 어플라이언스 또는 Panorama 가상 어플라이언스입니다. Panorama 모드의 M-시리즈 어플라이언스 또는

 ©2024 Palo Alto Networks, Inc.

Panorama 또는 레거시(ESXi 및 vCloud Air) 모드의 Panorama 가상 어플라이언스를 사용하여 전용 로그 수집기를 관리할 수 있습니다. 전용 로그 수집기를 관리하기 위해 Panorama 웹 인터페이스를 사용하려면 관리 수집기로 추가해야 합니다. 그렇지 않으면 전용 로그 수집기에 대한 관리 액세스는 사전 정의된 관리 사용자(*admin*) 계정을 사용하는 CLI를 통해서만 사용할 수 있습니다. 전용 로그 수집기는 추가 관리 사용자 계정을 지원하지 않습니다.

로그 수집기 유형 중 하나 또는 둘 다를 사용하여 환경에 가장 적합한 로깅 솔루션을 얻을 수 있습니다(로컬 및 분산 로그 수집 참조).

수집기 그룹은 단일 논리적 로그 수집 단위로 작동하는 1~16개의 관리 수집기입니다. 수집기 그룹에 전용 로그 수집기가 포함된 경우 Panorama는 각 로그 수집기의 모든 디스크와 그룹의 모든 로그 수집기에 걸쳐 로그를 균일하게 배포합니다. 이 배포는 사용 가능한 저장 공간을 최적화합니다. 로그 수집기가 로그를 수신할 수 있도록 하려면 수집기 그룹에 추가해야 합니다. 여러 로그 수집기를 수집기 그룹에 할당하여 로그 중복성을 활성화할 수 있습니다(여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항 참조). 수집기 그룹 구성은 그룹의 로그 수집기로 로그를 보낼 수 있는 관리되는 방화벽을 지정합니다.

로그 수집기 및 수집기 그룹을 구성하려면 로그 수집 관리를 참조하십시오.

로컬 및 분산 로그 수집

Panorama로의 로그 포워딩을 구성하기 전에 로컬 로그 수집기, 전용 로그 수집기 또는 둘 다를 사용할지 결정해야 합니다.

로컬 로그 수집기는 추가 하드웨어 또는 가상 머신 인스턴스가 필요하지 않기 때문에 배포하기 쉽습니다. 고가용성(HA) 구성에서는 두 Panorama 피어의 로컬 로그 수집기로 로그를 보낼 수 있습니다. 패시브 Panorama는 페일오버가 로그 수집을 시작할 때까지 기다리지 않습니다.

로컬 로그 수집의 경우 *Log Collector*를 논리적 컨테이너로 사용하지 않고 로그를 저장하는 레거시 모드의 *Panorama* 가상 어플라이언스에 로그를 포워딩할 수도 있습니다.

전용 로그 수집기는 M-700, M-600, M-500, M-300, M-200 또는 로그 수집기 모드의 Panorama 가상 어플라이언스입니다. 전용 로그 수집기는 방화벽 관리가 아닌 로그 수집만 하기 때문에 로컬 로그 수집기보다 더 강력한 환경을 허용합니다. 전용 로그 수집기는 다음과 같은 이점을 제공합니다.

- Panorama 관리 서버가 로깅 대신 관리 기능에 더 많은 리소스를 사용하도록 설정합니다.
- 전용 하드웨어 어플라이언스에 대용량 로그 스토리지를 제공합니다.
- 더 높은 로깅 속도를 활성화합니다.
- RAID 1 스토리지로 수평 확장성과 중복성을 제공합니다.
- 방화벽이 원격 Panorama 관리 서버보다 가까운 로그 수집기로 로그를 보내는 데 더 많은 대역폭을 사용할 수 있는 네트워크에서 대역폭 리소스를 최적화합니다.
- 지역 규정 요구 사항을 충족할 수 있습니다(예: 규정에 따라 특정 지역에서 로그가 나가는 것을 허용하지 않을 수 있음).

분산 로그 수집은 HA 구성의 Panorama 피어가 방화벽 및 전용 로그 수집기의 배포 및 구성을 관리하는 토폴로지를 보여줍니다.

Panorama 관리 서버는 *HA* 구성으로 배포할 수 있지만 전용 로그 수집기는 배포할 수 없습니다.

©2024 Palo Alto Networks, Inc.

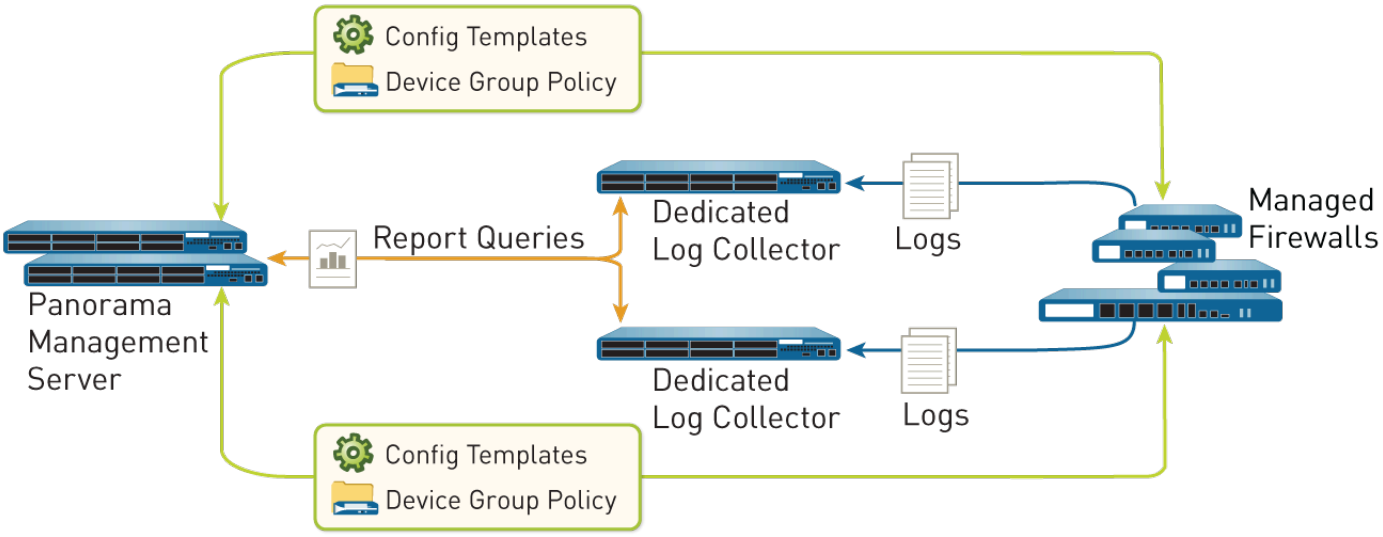


그림 **4:** 분산 로그 수집

여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항

여러 로그 수집기(최대 16개)로 수집기 그룹을 구성하여 로그 중복성을 보장하고 로그 보존 기간을 늘리며 단일 로그 수집기의 용량을 초과하는 로깅 속도를 수용할 수 있습니다(용량 정보는 Panorama 모델 참조). 모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 Panorama 모델인 모든 M-700 기기, 모든 M-600 기기, 모든 M-500 기기, 모든 M-300 기기, 모든 M-200 기기 또는 모든 Panorama 가상 어플라이언스에서 실행되어야 합니다. 예를 들어 단일 관리형 방화벽이 48TB의 로그를 생성하는 경우 해당 로그를 수신하는 수집기 그룹에는 M-300 어플라이언스인 로그 수집기가 3개 이상 필요하거나 M-700 어플라이언스 또는 유사한 리소스가 할당된 Panorama 가상 어플라이언스인 로그 수집기 1개가 필요합니다.

여러 Log Collector가 있는 Collector Group은 사용 가능한 저장 공간을 하나의 논리 단위로 사용하고 모든 Log Collector에 균일하게 로그를 배포합니다. 로그 배포는 로그 수집기(Panorama 모델 참조)의 디스크 용량과 로그를 소유하고 디스크에 쓰는 로그 수집기를 동적으로 결정하는 해시 알고리즘을 기반으로 합니다. Panorama는 기본 설정 목록을 사용하여 관리되는 방화벽이 로그를 전달할 수 있는 로그 수집기 목록의 우선 순위를 지정하지만 Panorama는 기본 설정 목록에 지정된 첫 번째 로그 수집기에 반드시 로그를 기록하지 않습니다. 예를 들어 다음 기본 설정 목록을 고려하십시오.

관리 방화벽	수집기 그룹에 정의된 로그 포워딩 기본 설정 목록
FW1	L1,L2,L3
FW2	L4,L5,L6

이 목록을 사용하여 FW1은 기본 로그 수집기를 사용할 수 있는 한 로그를 L1으로 전달합니다. 그러나 해시 알고리즘을 기반으로 Panorama는 디스크에 로그를 기록하는 소유자로 L2를 선택할 수 있습니다. L2에 액세스할 수 없게 되거나 샤시 오류가 발생하면 FW1은 L1에 계속 연결할 수 있기 때문에 알 수 없습니다.

©2024 Palo Alto Networks, Inc.

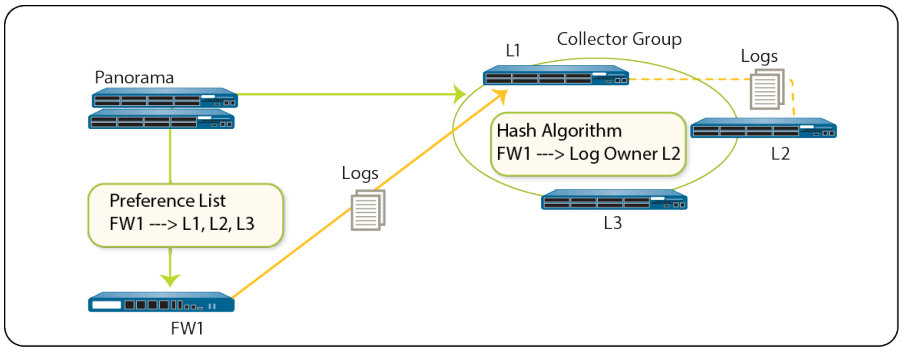


그림 **5:** 예 **-** 일반적인 로그 수집기 그룹 설정

Collector Group에 Log Collector가 하나만 있고 Log Collector에 장애가 발생하는 경우 방화벽은 해당 HDD/SSD에 로그를 저장합니다(사용 가능한 저장 공간은 방화벽 모델에 따라 다름). Log Collector에 대한 연결이 복원되는 즉시 방화벽은 오류가 발생하기 전에 중단된 로그 포워딩을 재개합니다.

여러 개의 로그 수집기가 있는 수집기 그룹의 경우 방화벽은 하나의 로그 수집기가 다운된 경우 로컬 저장소에 로그를 버퍼링하지 않습니다. L2가 다운된 예제 시나리오에서 FW1은 계속해서 L1에 로그를 보내고 L1은 L2에 보낼 로그 데이터를 저장합니다. L2가 백업되면 L1은 더 이상 L2에 대한 로그 데이터를 저장하지 않으며 예상대로 배포가 재개됩니다. Collector Group의 Log Collector 중 하나가 다운되면 다운된 Log Collector에 기록될 로그가 기본 설정 목록의 다음 Log Collector에 재배포됩니다.

*Palo Alto Networks*는 *1*개 로그 수집기가 다운될 경우 분할 브레인 및 로그 수집 문제를 방지하기 위해 수집기 그룹에 최소 *3*개의 로그 수집기를 추가할 것을 권장합니다. 자세한 내용은 기본 컬렉터 그룹 동작의 변경 사항을 참조하십시오.

한 수집기 그룹에서 *2*개의 로그 수집기가 지원되지만 한 로그 수집기가 다운되면 수집기 그룹이 작동하지 않습니다.

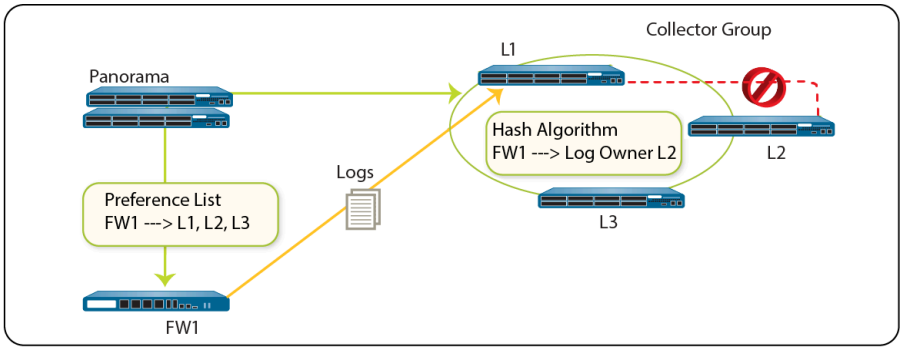


그림 **6:** 예 **-** 로그 수집기가 실패하는 경우

Palo Alto Networks는 수집기 그룹에서 여러 로그 수집기를 사용하는 경우 다음 완화 방법을 권장합니다.

- 수집기 그룹을 구성할 때 로그 중복을 활성화합니다. 이렇게 하면 수집기 그룹에서 하나의 로그 수집기를 사용할 수 없게 되는 경우에도 로그가 손실되지 않습니다. 각 로그에는 두 개의 사본이 있으며 각 사본은 다른 로그 수집기에 있습니다. 로그 중복성은 각 로그 수집기에 동일한 수의 로깅 디스크가 있는 경우에만 사용할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

중복을 활성화하면 더 많은 로그가 생성되기 때문에 이 구성에는 더 많은 저장 용량이 필요합니다. *Collector Group*의 공간이 부족하면 오래된 로그를 삭제합니다.

중복을 활성화하면 수집기 그룹에서 로그 처리 트래픽이 두 배로 늘어나 최대 로깅 속도가 절반으로 줄어듭니다. 각 로그 수집기는 수신하는 각 로그의 복사본을 배포해야 하기 때문입니다.

- Log Collector 오류가 발생할 경우 즉시 교체할 수 있도록 OSS(On-Site-Spare)를 확보하십시오.
- Panorama에 로그를 전달하는 것 외에도 외부 서비스에 대한 포워딩을 백업 스토리지로 구성합니다. 외부 서비스는 syslog 서버, 이메일 서버, SNMP 트랩 서버 또는 HTTP 서버일 수 있습니다.

로그 포워딩 옵션

기본적으로 각 방화벽은 로그 파일을 로컬에 저장합니다. 중앙 집중식 로그 모니터링 및 보고서 생성을 위해 Panorama를 사용하려면 Panorama로의 로그 포워딩을 구성해야 합니다. 로그를 전달하기 위해 전용 서비스 경로를 구성하지 않는 한 로그는 기본적으로 관리 인터페이스를 통해 전달됩니다. Panorama는 로그 수집기, Strata Logging Service 또는 둘 다에 대한 병렬 포워딩을 지원합니다. 방화벽이나 Panorama에서 직접 서비스로 로그를 포워딩하여 보관, 알림 또는 분석을 위해 외부 서비스를 사용할 수도 있습니다. 외부 서비스에는 syslog 서버, 이메일 서버, SNMP 트랩 서버 또는 HTTP 기반 서비스가 포함됩니다. 방화벽 로그를 포워딩하는 것 외에도 Panorama 관리 서버 및 로그 수집기가 생성하는 로그를 포워딩할 수 있습니다. Panorama 관리 서버, 로그 수집기 또는 로그를 포워딩하는 방화벽은 로그를 대상(syslog 메시지, 이메일 알림, SNMP 트랩 또는 HTTP 페이로드)에 적합한 형식으로 변환합니다.

Palo Alto Networks 방화벽 및 Panorama는 다음 로그 포워딩 옵션을 지원합니다. 옵션을 선택하기 전에 Panorama 모델의 로깅 용량을 고려하고 Panorama 로그 저장 요구 사항을 결정하십시오.

- 방화벽에서 Panorama로, Panorama에서 외부 서비스로 로그 포워딩 — 이 구성은 방화벽과 외부 서비스 간의 연결에 로깅 속도를 유지하기에 충분하지 않은 대역폭이 있는 배포에 가장 적합하며, 연결이 원격인 경우에 종종 이런 문제가 발생합니다. 이 구성은 일부 처리를 Panorama로 오프로드하여 방화벽 성능을 향상시킵니다.

로그를 다른 대상으로 포워딩하도록 각 수집기 그룹을 구성할 수 있습니다.

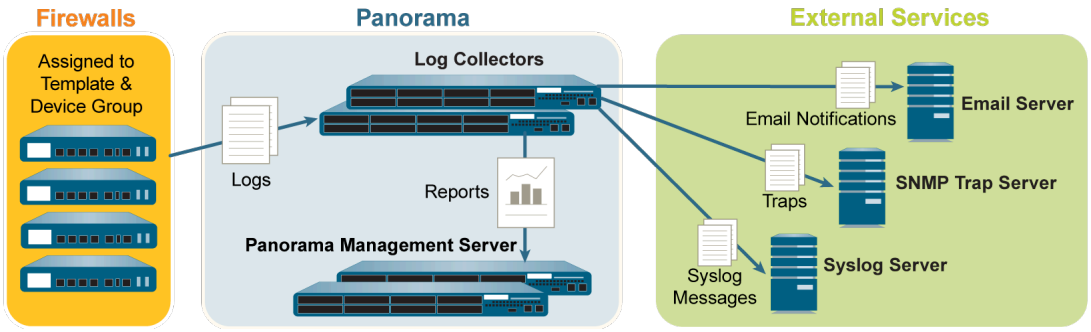


그림 **7: Panorama** 및 외부 서비스로의 로그 포워딩

- 방화벽에서 Panorama 및 외부 서비스로 로그를 병렬로 포워딩 — 이 구성에서 Panorama와 외부 서비스는 모두 별도의 로그 포워딩 플로우의 엔드포인트입니다. 방화벽은 외부 서비스에 로그를 포워딩하기

©2024 Palo Alto Networks, Inc.

위해 Panorama에 의존하지 않습니다. 이 구성은 방화벽과 외부 서비스 간의 연결에 로깅 속도를 유지하기에 충분한 대역폭이 있는 배포에 가장 적합하며, 이는 종종 연결이 로컬인 경우입니다.

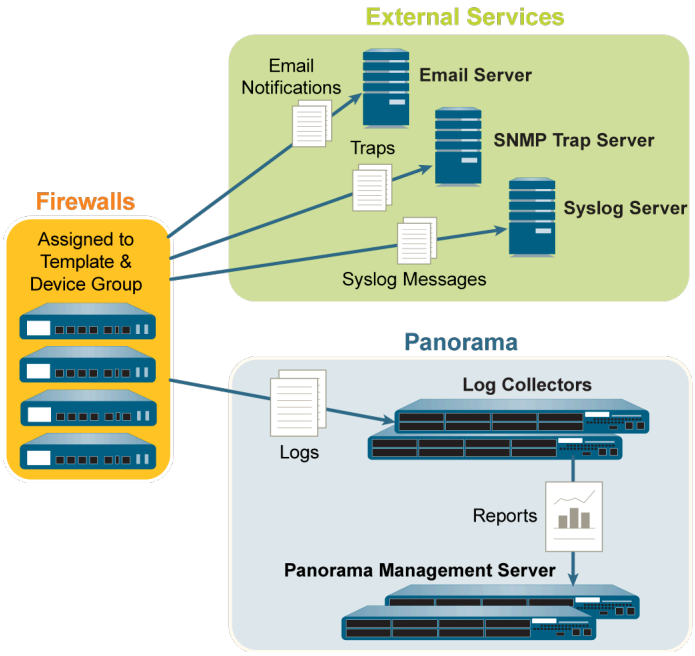


그림 **8:** 외부 서비스 및 **Panorama**에 병렬로 로그 포워딩

중앙 집중식 보고

Panorama는 관리되는 모든 방화벽의 로그를 집계하고 전체 네트워크에서 애플리케이션 사용, 사용자 활동 및 트래픽 패턴에 대한 글로벌 보기를 위해 집계된 데이터에 대한 보고를 가능하게 합니다. 방화벽이 Panorama에 추가되는 즉시 ACC는 네트워크를 통과하는 모든 트래픽을 표시할 수 있습니다. 로깅이 활성화된 상태에서 ACC의 로그 항목을 클릭하면 애플리케이션에 대한 세부 정보에 직접 액세스할 수 있습니다.

보고서 생성을 위해 Panorama는 로컬 Panorama 데이터베이스와 관리하는 원격 방화벽이라는 두 가지 소스를 사용합니다. Panorama 데이터베이스는 요약된 로그와 일부 세부 로그를 모두 저장하기 위해 할당된 Panorama의 로컬 저장소를 나타냅니다. 분산 로그 수집 배포가 있는 경우 Panorama 데이터베이스에는 Panorama의 로컬 스토리지와 모든 관리되는 로그 수집기가 포함됩니다. Panorama는 모든 관리 방화벽에서 15분 간격으로 수집된 정보(트래픽, 애플리케이션, 위협)를 요약합니다. 로컬 Panorama 데이터베이스를 사용하면 응답 시간이 빨라지지만 Panorama에 로그를 포워딩하지 않으려는 경우 Panorama에서 원격 방화벽에 직접 액세스하여 관리되는 방화벽에 로컬로 저장된 데이터에 대한 보고서를 실행할 수 있습니다.

Panorama는 그대로 사용할 수 있는 40개 이상의 사전 정의된 보고서를 제공하거나 저장할 수 있는 사용자 정의 보고서 및 보고서 그룹을 생성하기 위해 다른 보고서의 요소를 결합하여 사용자 정의할 수 있습니다. 보고서는 요청 시, 되풀이되는 일정으로 생성할 수 있으며 이메일 전송을 예약할 수 있습니다. 이러한 보고서는 사용자 및 컨텍스트에 대한 정보를 제공하므로 이벤트의 상관 관계를 파악하고 패턴, 추세 및 잠재적 관심 영역을 식별할 수 있습니다. 로깅 및 보고에 대한 통합 접근 방식을 통해 ACC는 동일한 이벤트와 관련된 여러 로그의 항목을 상호 연관시킬 수 있습니다.

자세한 내용은 네트워크 활동 모니터링를 참조하십시오.

©2024 Palo Alto Networks, Inc.

Panorama를 사용한 데이터 재배포

데이터 재배포를 사용하면 각 소스를 한 번만 구성하면 여러 데이터 유형을 필요한 만큼 많은 클라이언트에 재배포할 수 있습니다. 이렇게 하면 네트워크 요구 사항이 변경될 때 소스와 클라이언트를 쉽게 추가하거나 제거할 수 있도록 네트워크를 확장할 수 있습니다.

또한 데이터 재배포는 사용자가 지정하는 방화벽 또는 Panorama 관리 시스템에만 정보 유형을 재배포하여 세분성을 제공합니다. 서브넷, 범위 및 지역을 사용하여 네트워크 트래픽을 추가로 줄이고 디바이스 용량을 최대화할 수 있습니다.

Palo Alto Networks 방화벽의 주요 이점 중 하나는 정책을 시행하고 IP 주소 대신 사용자 이름과 태그를 기반으로 보고서를 생성할 수 있다는 것입니다. 대규모 네트워크의 과제는 정책을 시행하고 보고서를 생성하는 모든 방화벽에 모든 정책 규칙에 적용되는 매핑과 태그가 있는지 확인하는 것입니다. 또한 인증 정책을 시행하는 모든 방화벽에는 사용자 기반에 대해 완전하고 동일한 인증 타임스탬프 세트가 필요합니다. 사용자가 서비스 및 애플리케이션에 액세스하기 위해 인증할 때마다 개별 방화벽은 관련 타임스탬프를 기록하지만 일관성을 보장하기 위해 다른 방화벽과 자동으로 공유하지 않습니다. 데이터 재배포는 필요한 데이터를 재배포할 수 있게 하여 대규모 네트워크에서 이러한 문제를 해결합니다. 그러나 방화벽 간에 데이터를 재배포하기 위해 추가 연결을 설정하는 대신 Panorama 인프라를 활용하여 관리되는 방화벽에 데이터 재분배을(를) 합니다. 인프라에는 방화벽에서 Panorama에 이르기까지 계층에서 데이터를 재배포할 수 있는 기존 연결이 있습니다. 그러면 Panorama는 정책을 시행하고 보고서를 생성하는 방화벽에 정보를 재배포할 수 있습니다.

각 방화벽 또는 Panorama 관리 서버는 최대 100개의 재배포 지점에서 데이터를 수신할 수 있습니다. 재배포 지점은 다른 방화벽이나 Panorama 관리 서버일 수 있습니다. 그러나 Windows 기반 User-ID 에이전트를 사용하여 매핑을 수행하고 정보를 방화벽에 재배포할 수도 있습니다. 방화벽만 사용자 트래픽이 인증 정책 규칙과 일치할 때 인증 타임스탬프를 기록합니다.

©2024 Palo Alto Networks, Inc.

역할 기반 액세스 제어

RBAC(역할 기반 액세스 제어)를 사용하면 관리 사용자(관리자)의 권한과 책임을 정의할 수 있습니다. 모든 관리자는 역할 및 인증 방법을 지정하는 사용자 계정이 있어야 합니다. 관리 역할은(는) Panorama 및 방화벽 컨텍스트 내에서 특정 구성 설정, 로그 및 보고서에 대한 액세스를 정의합니다. 디바이스 그룹 및 템플릿 관리자의 경우 컨텍스트 전환을 통해 특정 디바이스 그룹, 템플릿 및 방화벽에 대한 액세스를 정의하는 액세스 도메인에 역할을 매핑할 수 있습니다. 각 액세스 도메인을 역할과 결합하여 조직의 기능적 또는 지역적 영역 간에 정보를 분리할 수 있습니다. 예를 들어 관리자가 데이터 센터 방화벽에 대한 활동을 모니터링하도록 제한할 수 있지만 해당 관리자가 테스트 랩 방화벽에 대한 정책을 설정하도록 허용할 수 있습니다. 기본적으로 모든 Panorama 어플라이언스(가상 어플라이언스 또는 M-시리즈 어플라이언스)에는 모든 기능 영역과 모든 디바이스 그룹, 템플릿 및 방화벽에 대한 전체 읽기-쓰기 액세스(운용 관리자 액세스)를 제공하는 사전 정의된 관리 계정(admin)이 있습니다. 각 관리자에 대해 Panorama가 사용자 액세스 자격 증명을 확인하는 방법을 결정하는 인증 프로파일을 정의할 수 있습니다.



모든 관리자에 대해 기본 계정을 사용하는 대신 *Panorama*의 관리 또는 보고 기능에 액세스해야 하는 각 사람에 대해 별도의 관리 계정을 만드는 것이 가장 좋습니다. 이를 통해 무단 구성 변경에 대해 더 나은 보안을 제공하고 *Panorama*에서 각 관리자의 작업을 기록하고 식별할 수 있습니다.

- 관리 역할
- 인증 프로필 및 시퀀스
- 액세스 도메인
- 관리 인증

관리 역할

조직의 보안 요구 사항, 네트워크에서 사용하는 기존 인증 서비스 및 필요한 관리 역할을 기반으로 관리자 계정을 구성합니다. 역할은 관리자가 사용할 수 있는 시스템 액세스 유형을 정의합니다. 조직의 보안 요구 사항에 따라 필요에 따라 광범위하게 또는 세부적으로 액세스를 정의하고 제한할 수 있습니다. 예를 들어 데이터 센터 관리자는 모든 디바이스 및 네트워킹 구성에 액세스할 수 있지만 보안 관리자는 보안 정책 정의만 제어할 수 있고 다른 주요 개인은 제한된 CLI 또는 XML API 액세스 권한을 가질 수 있다고 결정할 수 있습니다. 역할 유형은 다음과 같습니다.

- 동적 역할 - Panorama 및 관리 방화벽에 대한 액세스를 제공하는 기본 제공 역할입니다. 새로운 기능이 추가되면 Panorama는 동적 역할의 정의를 자동으로 업데이트합니다. 수동으로 업데이트할 필요가 없습니다. 다음 표에는 동적 역할과 관련된 액세스 권한이 나열되어 있습니다.

동적 역할	권한
운용 관리자	Panorama에 대한 전체 읽기-쓰기 액세스
운용 관리자(읽기 전용)	Panorama에 대한 읽기 전용 액세스

©2024 Palo Alto Networks, Inc.

동적 역할	권한
Panorama 관리자	다음 작업을 제외하고 Panorama에 대한 전체 액세스 권한: • Panorama 또는 방화벽 관리자 및 역할을 생성, 수정 또는 삭제합니다. • **Device** > **Setup** > 작업 페이지에서 구성 내보내기, 유효성 검사, 되돌리기, 저장, 로드 또는 가져오기. • **Panorama** 탭에서 예약된 구성 내보내기 기능을 구성합니다. • 기술 지원 파일 생성, 통계 덤프 파일 생성 및 핵심 파일 다운로드(**Panorama** > **Support**)

- 관리자 역할 프로필 - 웹 인터페이스, CLI 및 XML API의 기능 영역에 대한 보다 세분화된 액세스 제어를 제공하기 위해 사용자 지정 역할을 생성할 수 있습니다. 새 기능이 제품에 추가되면 해당 액세스 권한으로 역할을 업데이트해야 합니다. Panorama는 사용자 지정 역할 정의에 새 기능을 자동으로 추가하지 않습니다. 관리자 역할 프로파일 구성을(를) 수행할 때 다음 프로파일 유형 중 하나를 선택합니다.

관리자 역할 프로필	설명
Panorama	이러한 역할의 경우 Panorama 관리자 및 Panorama 역할의 관리를 제외하고 운용 관리자 동적 역할이 사용할 수 있는 모든 Panorama 기능에 대한 읽기-쓰기 액세스, 읽기 전용 액세스 또는 액세스 없음을 할당할 수 있습니다. 후자의 두 기능에 대해 읽기 전용 액세스 권한을 할당하거나 액세스 권한을 할당하지 않을 수 있지만 읽기-쓰기 액세스 권한은 할당할 수 없습니다. Panorama 역할의 사용 예는 Panorama의 보안 정책 정의, 로그 및 보고서에 액세스해야 하는 보안 관리자를 위한 것입니다. Custom Panorama 관리자 역할에는 다음과 같은 제한 사항이 있습니다. • **Reboot Panorama**(**Panorama** > **Setup** > **Operations**)에 액세스할 수 없음 • 기술 지원 파일 생성, 통계 덤프 파일 생성, 및 핵심 파일 다운로드에 대한 액세스 권한 없음(**Panorama** > **Support**)
디바이스 그룹 및 템플릿	이러한 역할에 대해 읽기-쓰기 액세스, 읽기 전용 액세스 또는 디바이스 그룹, 템플릿 및 방화벽 컨텍스트 내의 특정 기능 영역에 대한 액세스 없음을 할당할 수 있습니다. 이러한 역할을 액세스 도메인와(과) 결합하여 조직의 기능적 또는 지역적 영역 간에 정보를 분리할 수 있습니다. 디바이스 그룹 및 템플릿 역할에는 다음과 같은 제한 사항이 있습니다. • CLI 또는 XML API에 대한 액세스 권한 없음 • 구성 또는 시스템 로그에 액세스할 수 없음 • VM 정보 소스에 대한 액세스 권한 없음 • **Reboot Panorama**(**Panorama** > **Setup** > **Operations**)에 액세스할 수 없음

©2024 Palo Alto Networks, Inc.

관리자 역할 프로필	설명

	• 기술 지원 파일 생성, 통계 덤프 파일 생성, 및 핵심 파일 다운로드에 대한 액세스 권한 없음(**Panorama** > **Support**)
	• **Panorama** 탭에서 액세스는 다음으로 제한됩니다.
	  • 디바이스 배포 기능(읽기-쓰기, 읽기 전용 또는 액세스 불가)
	  • 관리자 계정에 지정된 디바이스 그룹(읽기-쓰기, 읽기 전용 또는 액세스 권한 없음)
	  • 관리자 계정에 지정된 템플릿 및 관리 방화벽(읽기 전용 또는 액세스 불가)
	이 역할의 예로는 특정 디바이스 그룹 및/또는 템플릿에 대한 웹 인터페이스의 디바이스 및 네트워크 구성 영역에 액세스해야 하는 운영 직원의 관리자가 있습니다.

인증 프로필 및 시퀀스

인증 프로필은 관리자가 Panorama에 액세스할 때 로그인 자격 증명을 확인하는 인증 서비스를 정의합니다. 서비스는 로컬 인증 또는 외부 인증 서비스일 수 있습니다. 일부 서비스((SAML, TACACS+ 및 RADIUS)는 Panorama 대신 외부 서버에서 관리 계정에 대한 인증 및 권한 부여를 모두 관리하는 옵션을 제공합니다. 인증 서비스 외에도 인증 프로필은 Kerberos SSO(Single Sign-On) 및 SAML SSO(Single Logout)와 같은 옵션을 정의합니다.

일부 네트워크에는 다양한 사용자 및 사용자 그룹에 대한 여러 데이터베이스(예: TACACS+ 및 LDAP)가 있습니다. 이러한 경우 관리자를 인증하려면 Panorama가 로그인하는 동안 관리자와 비교하는 인증 프로필의 순위 순서인 인증 순서를 구성하십시오. Panorama는 관리자가 성공적으로 인증될 때까지 각 프로필을 순서대로 확인합니다. 관리자는 시퀀스의 모든 프로필에 대해 인증이 실패한 경우에만 액세스가 거부됩니다.

액세스 도메인

액세스 도메인은 특정 디바이스 그룹 및 템플릿에 대한 관리 액세스를 제어하고 관리되는 방화벽의 웹 인터페이스로 컨텍스트를 전환하는 기능도 제어합니다. 액세스 도메인은 디바이스 그룹 및 템플릿 역할이 있는 관리자에게만 적용됩니다. 관리 역할을 액세스 도메인에 매핑하면 관리자가 Panorama에서 액세스하는 정보를 매우 세부적으로 제어할 수 있습니다. 예를 들어, 데이터 센터의 방화벽에 대한 모든 디바이스 그룹을 포함하는 액세스 도메인을 구성하고 해당 액세스 도메인을 데이터 센터 트래픽 모니터링이 허용되지만 방화벽 구성은 허용되지 않는 관리자에게 할당하는 시나리오를 고려하십시오. 이 경우 액세스 도메인을 모든 모니터링 권한을 활성화하지만 디바이스 그룹 설정에 대한 액세스를 비활성화하는 역할에 매핑합니다. 또한 디바이스 그룹 및 템플릿 관리자는 구성 및 시스템 로그 보기, 구성 감사 수행, 보류 중인 작업 검토와 같은 액세스 도메인에서 관리되는 방화벽에 대한 관리 작업을 수행하고 재부팅, 기술 지원 파일 생성, 통계 덤프 실행 및 코어 파일 내보내기를 수행할 수 있습니다.

로컬 Panorama 구성에서 액세스 도메인을 구성한 다음 관리 계정 및 역할에 할당합니다. 로컬에서 할당을 수행하거나 외부 SAML, TACACS+ 또는 RADIUS 서버를 사용할 수 있습니다. 외부 서버를 사용하면 Panorama에서 설정을 재구성하는 대신 디렉토리 서비스를 통해 액세스 도메인을 빠르게 재할당할 수 있습니다. 외부 서버를 사용하려면 Panorama가 서버에 액세스할 수 있도록 하는 서버 프로필을 정의해야 합

 ©2024 Palo Alto Networks, Inc.

니다. 또한 RADIUS 또는 TACACS+ 서버에서 VSA(Vendor-Specific Attributes)를 정의하거나 SAML IdP 서버에서 SAML 속성을 정의해야 합니다.

예를 들어 RADIUS 서버를 사용하는 경우 각 관리자에 대해 VSA 번호와 값을 정의합니다. 정의된 값은 Panorama에 구성된 액세스 도메인과 일치해야 합니다. 관리자가 Panorama에 로그인을 시도하면 Panorama는 RADIUS 서버에 관리자 액세스 도메인 및 속성 번호를 쿼리합니다. RADIUS 서버의 응답에 따라 관리자는 액세스 권한이 부여되며 액세스 도메인에 할당된 방화벽, 가상 시스템, 디바이스 그룹 및 템플릿으로 제한됩니다.

관련 절차는 다음을 참조하십시오.

- 액세스 도메인 구성.
- Panorama 관리자를 위한 RADIUS 인증 구성.
- Panorama 관리자를 위한 TACACS+ 인증 구성.
- Panorama 관리자를 위한 SAML 인증 구성.

관리 인증

Panorama 관리자에 대해 다음 유형의 인증 및 권한 부여(관리 역할 및 액세스 도메인)를 구성할 수 있습니다.

인증 방법	권한 부여 방법	설명
로컬	로컬	관리 계정 자격 증명 및 인증 메커니즘은 Panorama에 로컬입니다. Panorama를 사용하여 계정에 관리 역할 및 액세스 도메인을 할당합니다. 계정을 더욱 안전하게 보호하기 위해 암호의 유효 기간을 정의하는 암호 프로필을 생성하고 Panorama 전체 암호 복잡성 설정을 지정할 수 있습니다. 자세한 내용은 Panorama 관리자에 대한 로컬 또는 외부 인증 구성을 참조하십시오.
SSH 키	로컬	관리 계정은 Panorama에 대해 로컬이지만 CLI에 대한 인증은 SSH 키를 기반으로 합니다. Panorama를 사용하여 계정에 관리 역할 및 액세스 도메인을 할당합니다. 자세한 내용은 CLI에 대한 SSH 키 기반 인증을 사용하여 관리자 구성을 참조하십시오.
인증서	로컬	관리 계정은 Panorama에 로컬이지만 웹 인터페이스에 대한 인증은 클라이언트 인증서를 기반으로 합니다. Panorama를 사용하여 계정에 관리 역할 및 액세스 도메인을 할당합니다. 자세한 내용은 웹 인터페이스에 대한 인증서 기반 인증으로 Panorama 관리자 구성을 참조하십시오.
외부 서비스	로컬	Panorama에서 로컬로 정의하는 관리 계정은 외부 Multi-Factor Authentication, SAML, Kerberos, TACACS+, RADIUS 또는 LDAP 서버에 정의된 계정에 대한 참조 역할을 합니다. 외부 서버가 인증을 수행합니다. Panorama를 사용하여 계정에 관리 역할 및 액세스 도메인을 할당합니다. 자세한 내용은 Panorama 관리자에 대한 로컬 또는 외부 인증 구성을 참조하십시오.

©2024 Palo Alto Networks, Inc.

인증 방법	권한 부여 방법	설명
외부	외부 서비스	관리 계정은 외부 SAML, TACACS+ 또는 RADIUS 서버에서만 정의됩니다. 서버는 인증과 권한 부여를 모두 수행합니다. 인증을 위해 TACACS+ 또는 RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하거나 SAML 서버에서 SAML 속성을 정의합니다. Panorama는 속성을 Panorama에서 정의한 관리자 역할 및 액세스 도메인에 매핑합니다. 자세한 내용은 다음을 참조하세요. • Panorama 관리자를 위한 SAML 인증 구성 • Panorama 관리자를 위한 TACACS+ 인증 구성 • Panorama 관리자를 위한 RADIUS 인증 구성

©2024 Palo Alto Networks, Inc.

Panorama 커밋, 검증 및 미리보기 작업

Panorama의 후보 구성에 대한 변경 사항을 활성화하거나 Panorama가 관리하는 디바이스(방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터)에 변경 사항을 푸시할 준비가 되면 구성 변경 사항 미리보기, 검증 또는 커밋을(를) 할 수 있습니다. 예를 들어 Panorama 구성에 Log Collector를 추가하면 Panorama에 대한 변경 사항을 커밋한 다음 Log Collector가 포함된 Collector Group에 변경 사항을 푸시할 때까지 방화벽이 해당 Log Collector에 로그를 보낼 수 없습니다.

관리자 또는 위치별로 변경 사항을 필터링한 다음 해당 변경 사항만 커밋, 푸시, 유효성 검사 또는 미리보기를 할 수 있습니다. 위치는 특정 디바이스 그룹, 템플릿, 수집기 그룹, 로그 수집기, 공유 설정 또는 Panorama 관리 서버일 수 있습니다.

변경 사항을 커밋하면 실행 중인 구성의 일부가 됩니다. 커밋하지 않은 변경 사항은 후보 구성의 일부입니다. Panorama는 이전 커밋이 진행 중인 동안 새 커밋을 시작할 수 있도록 커밋 요청을 대기열에 넣습니다. Panorama는 시작된 순서대로 커밋을 수행하지만 Panorama에서 시작한 자동 커밋(예: FQDN 새로 고침)에 우선 순위를 둡니다. 그러나 대기열에 이미 관리자가 시작한 최대 커밋 수(10)가 있는 경우 Panorama에서 보류 중인 커밋 처리를 완료한 후 새 커밋을 시작해야 합니다. Panorama 작업 관리자 사용(Tasks)하여 보류 중인 커밋을 취소하거나 보류, 진행 중, 완료 또는 실패한 커밋에 대한 세부 정보를 볼 수 있습니다. 커밋이 활성화될 변경 사항을 확인하려면 커밋 미리보기를 실행할 수 있습니다.

커밋을 시작하면 Panorama는 변경 사항을 활성화하기 전에 변경 사항의 유효성을 확인합니다. 검증 출력은 커밋을 차단하는 조건(오류) 또는 알아야 할 중요한 조건(경고)을 표시합니다. 예를 들어 유효성 검사는 커밋이 성공하기 위해 수정해야 하는 잘못된 경로 대상을 나타낼 수 있습니다. 확인 프로세스를 통해 커밋하기 전에 오류를 찾아 수정할 수 있습니다(실행 중인 구성은 변경되지 않음). 이것은 고정된 커밋 창이 있고 커밋이 오류 없이 성공하는지 확인하려는 경우에 유용합니다.

구성 커밋을 미리 볼 때 기존의 다른 기존 개체 사이에 추가된 모든 구성 개체는 추가된 구성 개체가 아닌 수정된 구성 개체로 표시됩니다. 예를 들어, `Address1` 및 `Address2`는 기존 주소 개체입니다. Panorama 관리자는 나중에 `Address3#` 만들고 `Address1`과 `Address2` 사이에 Address 개체를 추가합니다. Panorama 관리자가 구성 변경 사항을 미리 보기 위해 이동하면 `Address3`이 수정된 구성 개체로 표시됩니다.

자동 커밋 복구는 기본적으로 활성화되어 있어 관리되는 방화벽이 Panorama에서 푸시된 구성을 로컬로 테스트하여 새 변경 사항으로 인해 Panorama와 관리되는 방화벽 간의 연결이 끊어지지 않는지 확인할 수 있습니다. 커밋된 구성이 Panorama와 관리되는 방화벽 간의 연결을 끊으면 방화벽이 자동으로 커밋에 실패하고 구성이 이전 실행 구성으로 되돌려지며 공유 정책 또는 템플릿 상태(**Panorama** > **Managed Devices** > **Summary**)가 푸시된 구성 개체에 따라 동기화되지 않습니다. 또한 관리형 방화벽은 60분마다 Panorama에 대한 연결을 테스트하고 관리형 방화벽이 더 이상 Panorama에 성공적으로 연결할 수 없음을 감지하면 구성을 이전 실행 구성으로 되돌립니다.

©2024 Palo Alto Networks, Inc.

후보 구성 및 실행 중인 구성에 대한 자세한 내용은 Panorama 및 방화벽 구성 백업 관리을(를) 참조하십시오.

여러 관리자가 동시 세션 동안 구성을 변경하지 못하도록 하려면 구성 변경 제한을 위한 잠금 관리을(를) 참조하십시오.

관리 방화벽에 구성을 푸시할 때 *Panorama*는 실행 중인 구성을 푸시합니다. 이 때문에 *Panorama*에서는 변경 사항을 *Panorama*에 처음 커밋할 때까지 관리 방화벽에 변경 사항을 푸시할 수 없습니다.

©2024 Palo Alto Networks, Inc.

Panorama 배포 계획

- 관리 방식을 결정합니다. Panorama를 사용하여 정책을 중앙에서 구성 및 관리하고, 소프트웨어, 콘텐츠 및 라이선스 업데이트를 중앙에서 관리하고, 네트워크의 관리되는 방화벽에서 로깅 및 보고를 중앙 집중화할 계획입니까?

  네트워크에 Palo Alto Networks 방화벽을 이미 배포 및 구성한 경우 방화벽을 중앙 집중식 관리로 전환할지 여부를 결정합니다. 이 프로세스를 수행하려면 방화벽에서 Panorama로 모든 구성 및 정책을 마이그레이션해야 합니다. 자세한 내용은 방화벽을 Panorama 관리로 전환을 참조하십시오.

- Panorama 및 방화벽 소프트웨어 버전을 확인합니다. Panorama는 Panorama 버전과 일치하거나 Panorama 버전보다 이전인 PAN-OS 버전을 실행하는 방화벽을 관리할 수 있습니다. 자세한 내용은 Panorama 관리 호환성을 참조하십시오.

- (Multi-VSYS 방화벽) 네트워크에 Multi-VSYS Palo Alto Networks 방화벽을 이미 배포하고 구성한 경우 Palo Alto Networks는 Panorama에서 Multi-VSYS 방화벽의 모든 vsys 구성을 전환하고 관리할 것을 권장합니다. 이는 Multi-VSYS 방화벽에서 커밋 문제를 방지하는 데 필요하며 Panorama에서 최적화된 공유 개체 푸시의 이점을 활용할 수 있도록 해줍니다.

- (Multi-VSYS 방화벽) Panorama 공유 구성의 개체와 이름이 동일한 로컬로 구성된 방화벽 공유 개체를 삭제하거나 이름을 바꿉니다. 그렇지 않으면 업그레이드 후 Panorama의 구성 푸시가 실패하고 `<object-name> ## ## #` 오류가 표시됩니다.

- Panorama와 해당 관리 디바이스 및 고가용성 피어 간의 인증 방법을 결정합니다. 기본적으로 Panorama는 사전 정의된 인증서를 사용하여 관리 및 디바이스 간 통신에 사용되는 SSL 연결을 인증합니다. 그러나 사용자 지정 인증서 기반 인증을 구성하여 Panorama, 방화벽 및 로그 수집기 간의 SSL 연결 보안을 강화할 수 있습니다. 사용자 지정 인증서를 사용하면 Panorama와 Panorama가 관리하는 디바이스 간의 상호 인증을 보장하기 위해 고유한 신뢰 체인을 설정할 수 있습니다. 엔터프라이즈 PKI(공개 키 인프라)에서 인증서를 가져오거나 Panorama에서 생성할 수 있습니다.

- 고가용성 구성에서 Panorama를 사용할 계획입니다. 활성/수동 고가용성 쌍으로 설정합니다. Panorama 고가용성을 참조하십시오.

- 대규모 배포에서 네트워크 세분화 및 보안 요구 사항을 수용하는 방법을 계획합니다. 기본적으로 M-시리즈 어플라이언스에서 실행되는 Panorama는 Panorama에 대한 관리 액세스 및 디바이스(방화벽, Log Collectors, WildFire 어플라이언스 및 어플라이언스 클러스터) 관리, 로그 수집, Collector Group과의 통신, 디바이스에 소프트웨어 및 콘텐츠 업데이트 배포를 위해 관리(MGT) 인터페이스를 사용합니다. 그러나 보안을 강화하고 네트워크 분할을 활성화하기 위해 관리 액세스를 위해 MGT 인터페이스를 예약하고 다른 서비스에 대해 전용 M-시리즈 어플라이언스 인터페이스(Eth1, Eth2, Eth3, Eth4 및 Eth5)를 사용할 수 있습니다.

- 네트워크 활동에 대한 의미 있는 보고를 위해 로깅 솔루션을 계획하십시오.

  - AWS 또는 Azure에서 Log Collector 모드로 배포된 Panorama 가상 어플라이언스에 대한 리소스 할당을 확인합니다. Panorama 가상 어플라이언스는 크기가 조정된 경우 로그 수집기 모드를 유지하지 않습니다. 이로 인해 로그 데이터가 손실됩니다.
  - 네트워크가 보안 및 규정 준수 요구 사항을 충족하는 데 필요한 로그 스토리지 용량을 예측합니다. Panorama 모델의 로깅 용량, 네트워크 토폴로지, 로그를 보내는 방화벽 수, 로그 트래픽 유형(예: URL 필터링 및 위협 로그 대 트래픽 로그), 방화벽이 로그를 생성하는 속도 및 Panorama에 로그를 저장하려는 일 수와 같은 요소를 고려하십시오. 자세한 내용은 Panorama 로그 스토리지 요구 사항 결정을 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

- Panorama 외에 외부 서비스(예: syslog 서버)에 로그를 포워딩해야 합니까? 로그 포워딩 옵션을 참조하십시오.
- 온프레미스에서 자체 로그 스토리지를 소유하거나 관리하고 싶습니까? 아니면 Palo Alto Networks에서 제공하는 Strata Logging Service를 활용하고 싶습니까?
- 장기 스토리지 솔루션이 필요한 경우 로그를 포워딩할 수 있는 Splunk 또는 ArcSight와 같은 SIEM(보안 정보 및 이벤트 관리) 솔루션이 있습니까?
- 로깅에 중복성이 필요합니까?

  여러 로그 수집기가 있는 수집기 그룹을 구성하는 경우 하나의 로그 수집기를 사용할 수 없게 되는 경우에도 로그가 손실되지 않도록 중복성을 활성화할 수 있습니다(여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항 참조).

  HA 구성의 레거시 모드에서 Panorama 가상 어플라이언스를 배포하는 경우 관리되는 방화벽은 각 로그의 복사본이 각 피어에 있도록 두 HA 피어 모두에 로그를 보낼 수 있습니다. 이 중복성 옵션은 기본적으로 활성화되어 있습니다(로그 포워딩 및 버퍼링 기본값 수정 참조).
- NFS(네트워크 파일 시스템)에 로그인하시겠습니까? Panorama 가상 어플라이언스가 레거시 모드이고 전용 로그 수집기를 관리하지 않는 경우 NFS 스토리지는 로그 스토리지 용량을 8TB 이상으로 늘릴 수 있는 유일한 옵션입니다. NFS 스토리지는 Panorama가 ESXi 서버에서 실행되는 경우에만 사용할 수 있습니다. NFS 스토리지를 사용하는 경우 방화벽은 HA 쌍의 기본 피어에만 로그를 보낼 수 있습니다. 기본 피어만 NFS에 마운트되고 쓸 수 있습니다.

- 관리자가 관리 방화벽 및 Panorama에 액세스하는 데 필요한 역할 기반 액세스 권한을 결정합니다. Panorama에 대한 관리 액세스 설정을 참조하십시오.
- 필요한 디바이스 그룹을 계획합니다. 기능, 보안 정책, 지리적 위치 또는 네트워크 분할을 기반으로 방화벽을 그룹화할지의 여부를 고려합니다. 기능 기반 디바이스 그룹의 예로는 연구 개발 팀에서 사용하는 모든 방화벽이 포함된 그룹이 있습니다. 공통성을 기반으로 더 작은 디바이스 그룹을 만들지, 더 쉽게 확장할 수 있는 더 큰 디바이스 그룹을 만들지 또는 복잡한 관리 계층을 단순화하기 위해 디바이스 그룹 계층을 만들지 고려하십시오.
- 정책 관리를 위한 계층화 전략을 계획합니다. 방화벽이 디바이스 그룹 계층 내에서 정책 규칙을 상속 및 평가하는 방법과 네트워크 요구 사항을 충족하기 위해 공유 규칙, 디바이스 그룹 규칙 및 방화벽별 규칙을 가장 잘 구현하는 방법을 고려하십시오. 가시성 및 중앙 집중식 정책 관리를 위해 공유 또는 디바이스 그룹 규칙에 대한 방화벽별 예외가 필요한 경우에도 규칙 관리에 Panorama를 사용하는 것이 좋습니다. 필요한 경우 디바이스 그룹 내의 방화벽 하위 집합에 정책 규칙을 푸시할 수 있습니다.
- 템플릿 및 템플릿 스택(template stack)에서 네트워크 구성 설정을 상속하는 방법을 기반으로 방화벽 구성을 계획합니다. 예를 들어 하드웨어 모델, 지리적 근접성 및 표준 시간대, DNS 서버 및 인터페이스 설정에 대한 유사한 네트워크 요구 사항을 기반으로 템플릿에 방화벽을 할당하는 것을 고려하십시오.

©2024 Palo Alto Networks, Inc.

Panorama 배포: 작업 개요

다음 작업 목록에는 Panorama를 시작하는 단계가 요약되어 있습니다. 중앙 관리를 위해 Panorama를 사용하는 방법의 예는 사용 사례: Panorama를 사용하여 방화벽 구성을(를) 참조하십시오.

STEP 1 | (M-시리즈 기기만 해당) 기기를 랙에 장착합니다.

STEP 2 | Panorama에 대한 네트워크 액세스를 활성화하려면 초기 구성을 수행하십시오. Panorama 가상 어플라이언스 설정 또는 M-시리즈 어플라이언스 설정을(를) 참조하십시오.

STEP 3 | Panorama 등록 및 라이선스 설치.

STEP 4 | Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 5 | (권장) 고가용성 구성에서 Panorama를 설정합니다. Panorama 고가용성를 참조하십시오.

STEP 6 | 관리되는 디바이스로 방화벽 추가.

STEP 7 | 디바이스 그룹 추가 또는 디바이스 그룹 계층 생성, 템플릿 추가 및 (해당되는 경우) 템플릿 스택(template stack) 구성.

STEP 8 | (선택 사항) Panorama 및/또는 외부 서비스로의 로그 포워딩을 구성합니다. 로그 수집 관리를 참조하십시오.

STEP 9 | Panorama에서 가시성 및 보고 도구를 사용하여 네트워크 활동 모니터링.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

Panorama 설정

네트워크의 모든 방화벽에서 중앙 집중식 보고 및 응집력 있는 정책 관리를 위해 Panorama™ 관리 서버를 가상 어플라이언스 또는 하드웨어 어플라이언스(M-200, M-300, M-500, M-600 또는 M-700 어플라이언스)로 배포할 수 있습니다.

다음 주제에서는 네트워크에서 Panorama를 설정하는 방법에 대해 설명합니다.

- Panorama 로그 스토리지 요구 사항 결정
- 대규모 방화벽 배포 관리
- Panorama 가상 어플라이언스 설정
- M-시리즈 어플라이언스 설정
- Panorama 등록 및 라이선스 설치
- Panorama 디바이스 인증서 설치
- 전용 로그 수집기에 대한 디바이스 인증서 설치
- 다른 Panorama 모델로 전환
- Panorama 관리 인터페이스 액세스 및 탐색
- Panorama에 대한 관리 액세스 설정
- 사용자 지정 인증서를 사용하여 인증 설정

Panorama 로그 스토리지 요구 사항 결정

Panorama 배포를 계획할 때, Panorama에서 Panorama 모델 배포에 필요한 로그 스토리지 용량이 어느 정도인지, 해당 어플라이언스의 스토리지를 기본 용량 이상으로 확장할지, 전용 로그 수집기를 배포할지, 로그 포워딩을 Panorama에서 외부 목적지로 구성할지에 대해 추정합니다. 로그 스토리지가 최대 용량에 도달하면 Panorama는 이전 로그를 자동으로 삭제하여 새 로그를 위한 공간을 생성합니다.

Panorama에 필요한 대략적인 로그 스토리지를 결정하려면 다음 단계를 수행하십시오. 자세한 내용 및 사용 사례는 Panorama 크기 조정 및 디자인 가이드를 참조하세요.

STEP 1 | 조직의 로그 보존 요구 사항을 결정합니다.

로그 보존 요구 사항에 영향을 미치는 요소는 다음과 같습니다.

- 조직의 IT 정책
- 로그 중복 - 수집기 그룹을 구성할 때 로그 중복을 활성화하면 각 로그에 두 개의 복사본이 포함되어 필요한 로그 저장 용량이 두 배가 됩니다.
- PCI DSS(Payment Card Industry Data Security Standard), Sarbanes-Oxley 법 및 HIPAA(Health Insurance Portability and Accountability Act)에서 지정한 것과 같은 규제 요구 사항.



조직에서 일정 기간 후 로그를 제거해야 하는 경우 로그 유형별로 만료 기간을 설정할 수 있습니다. 유형별로 로그 보존의 우선 순위를 지정해야 하는 경우 각 로그 유형에 대한 스토리지 할당량을 총 공간의 백분율로 설정할 수도 있습니다. 자세한 내용은 로그 및 보고서에 대한 저장소 할당량 및 만료 기간 관리를 참조하십시오.

©2024 Palo Alto Networks, Inc.

STEP 2 | 평균 일일 로깅 속도를 결정합니다.

피크 시간과 피크 시간이 아닌 시간에 매일 여러 번 이 작업을 수행하여 평균을 추정합니다. 요율을 더 자주 샘플링할수록 추정치가 더 정확해집니다.

1. 현재 로그 생성 속도를 초당 로그로 표시합니다.
   - Panorama가 아직 로그를 수집하지 않는 경우 각 방화벽의 CLI에 액세스하여 다음 명령을 실행하고 모든 방화벽에 대한 총 속도를 계산합니다. 이 명령은 마지막 1초 동안 수신된 로그 수를 표시합니다.

     ```
     > debug log-receiver statistics
     ```

   - Panorama가 이미 로그를 수집하는 경우 로그를 수신하는 각 어플라이언스(Panorama 관리 서버 또는 전용 로그 수집기)의 CLI에서 다음 명령을 실행하고 총 비율을 계산합니다. 이 명령은 지난 5분 동안의 평균 로깅 속도를 제공합니다.

     ```
     > debug log-collector log-collection-stats show incoming-logs
     ```

     또한 *SNMP* 관리자를 사용하여 로그 수집기*(panLogCollector MIB, OID 1.3.6.1.4.1.25461.1.1.6* 참조*)* 및 방화벽*(panDeviceLogging, OID 1.3.6.1.4.1.25461.2.1.2* 참조*)*의 로깅 속도를 결정할 수 있습니다. *7).*
2. 샘플링된 비율의 평균을 계산합니다.
3. 초당 평균 로그에 86,400을 곱하여 일일 로깅 속도를 계산합니다.

STEP 3 | 필요한 저장 용량을 예상합니다.

이 공식은 추정치를 제공합니다. 필요한 스토리지의 정확한 양은 공식 결과와 다릅니다.

공식을 사용하십시오.

[(<logs_per_second> x 86400) x <days_of retention>] x <average_log_size> ÷ (1024 x 1024 x 1024)

평균 로그 크기는 로그 유형에 따라 크게 다릅니다. 하지만 489바이트를 대략적인 평균 로그 크기로 사용할 수 있습니다.

예를 들어, Panorama가 로그 속도가 1,500LPS인 30일 동안 로그를 저장해야 하는 경우 필요한 로그 저장 용량은 **[(1500 x 86400) x 30] x 489 ÷ (1024 x 1024 x 1024) = 1770GB**입니다.

위의 결과는 기본 할당량 설정이 세부 로그에 대해 사용 가능한 스토리지의 60%를 예약한 세부 로그에 대한 계산입니다. 즉, 계산된 숫자는 로그 수집기가 사용하는 스토리지의 60%를 나타냅니다. 필요한 총 스토리지를 계산하려면 이 숫자를 0.60으로 나눕니다. **1770 ÷ 0.6 = 2951GB**.

사용 가능한 디스크 공간의 1/3인 약 33%는 업그레이드, 다운그레이드를 지원하고 데이터베이스 손상 수정을 지원하기 위해 logd 형식의 로그에 할당됩니다. 총 스토리지를 계산하려면 필요한 스토리지를 0.66으로 나눕니다. **2951 ÷ 0.66 =** 총 **4471** 스토리지 수.

©2024 Palo Alto Networks, Inc.

STEP 4 | 다음 단계...

Panorama에 더 많은 로그 스토리지 용량이 필요하다고 판단되는 경우:

- Panorama 가상 어플라이언스에서 로그 스토리지 용량을 확장합니다.
- M-시리즈 어플라이언스의 스토리지를 늘립니다.

©2024 Palo Alto Networks, Inc.

대규모 방화벽 배포 관리

Panorama™는 대규모 방화벽 배포를 관리하기 위한 여러 옵션을 제공합니다. 모든 관리 기능을 통합하기 위해 Panorama는 관리 전용 모드에서 ESXi의 M-600, M-700 어플라이언스 또는 Panorama 가상 어플라이언스를 사용하여 최대 5,000개의 방화벽을 관리하거나 관리 전용 모드에서 Panorama 가상 어플라이언스를 사용하여 최대 2,500개의 방화벽 관리를 지원합니다. 5,000개 이상의 방화벽이 있는 대규모 방화벽 배포의 배포 및 운영 관리를 단순화하기 위해 Panorama Interconnect 플러그인을 사용하면 단일 Panorama 컨트롤러에서 여러 Panorama 관리 서버 노드를 관리할 수 있습니다.

- 최적의 대규모 방화벽 배포 솔루션 결정
- M-시리즈 및 Panorama 가상 어플라이언스를 위한 디바이스 관리 용량 증가

최적의 대규모 방화벽 배포 솔루션 결정

대규모 방화벽 배포 구성을 관리하는 운영상의 부담을 줄이기 위해 Palo Alto Networks는 배포 시나리오에 가장 적합한 다양한 방화벽 관리 옵션을 제공합니다.

대규모 방화벽 배포가 하나 또는 매우 적은 수의 Panorama 관리 서버로 구성된 경우 ESXi에 M-600, M-700 어플라이언스 또는 Panorama 가상 어플라이언스를 배포하여 최대 5,000개의 방화벽을 관리하거나 Panorama 가상 어플라이언스를 배포하여 최대 2,500개의 방화벽을 관리함으로써 단일 Panorama 관리 서버에서 모든 Panorama 기능을 활용할 수 있습니다. M-시리즈 및 Panorama 가상 어플라이언스를 위한 디바이스 관리 용량 증가은(는) 더 적은 수의 방화벽을 관리하기 위해 여러 Panorama 관리 서버를 배포하는 대신 단일 Panorama 관리 서버에서 많은 수의 방화벽을 관리하는 수직 확장 배포에 이상적입니다.

대규모 방화벽 배포가 유사한 구성의 여러 Panorama 관리 서버로 구성된 경우 Panorama Interconnect 플러그인을 사용하면 단일 Panorama 컨트롤러에서 여러 Panorama 노드를 관리할 수 있습니다. 이 플러그인은 Panorama Controller에서 정책 및 구성을 중앙에서 관리할 수 있기 때문에 대규모 방화벽 배포의 배포 및 운영 관리를 단순화합니다. Panorama 컨트롤러에서 디바이스 그룹 및 템플릿 스택(template stack) 구성이 Panorama 노드와 동기화되고 관리되는 디바이스로 푸시됩니다. Panorama Interconnect 플러그인은 여러 대의 분산 Panorama 관리 서버가 있는 수평 확장 방화벽 배포에 이상적입니다.

M-시리즈 및 Panorama 가상 어플라이언스를 위한 디바이스 관리 용량 증가

VMware ESXi에 설치된 단일 M-600, M-700 어플라이언스 또는 Panorama™ 가상 어플라이언스로 최대 5,000개의 방화벽을 관리하거나, 지원되는 다른 모든 Panorama 가상 어플라이언스로 최대 2,500개의 방화벽을 관리하여 대규모 방화벽 배포의 관리 공간을 줄일 수 있습니다.

- 디바이스 관리 용량 요구 사항 증가
- 디바이스 관리 용량 증가를 위한 Panorama 설치

디바이스 관리 용량 요구 사항 증가

VMware ESXi에 설치된 단일 M-600, M-700 어플라이언스 또는 Panorama™ 가상 어플라이언스로 최대 5,000개의 방화벽을 관리하거나, 지원되는 다른 모든 Panorama 가상 어플라이언스로 최대 2,500개의 방화벽을 관리할 수 있습니다. 단일 Panorama 관리 서버에서 이러한 대규모 배포를 관리하면 구성 관리의

©2024 Palo Alto Networks, Inc.

운영 복잡성이 완화되고 여러 Panorama 관리 서버를 관리하는 데 따르는 보안 및 규정 준수 위험이 줄어듭니다.

로그 수집의 경우 단일 Panorama 관리 서버가 각 개별 Panorama 관리 서버에 액세스할 필요 없이 관리되는 디바이스의 로그 데이터를 보고 분석할 수 있는 중앙 위치를 제공하기 때문에 이상적입니다. 시스템 또는 네트워크 장애 발생 시 이중화를 제공하기 위해 Palo Alto Networks는 고가용성(HA) 구성에서 두 개의 Panorama 관리 서버를 배포할 것을 권장합니다. Panorama 시스템 및 구성 로그의 경우 최소 92GB 용량의 추가 디스크가 필요합니다. 이 추가 디스크는 Panorama가 재부팅되고 시스템 및 구성 로그 저장소의 파티션으로 마운트될 때 Panorama 가상 어플라이언스에서 자동으로 감지됩니다.

사전 정의된 보고서를 생성하려면 사전 정의된 보고서에 Panorama 데이터를 사용하도록 Panorama를 활성화해야 합니다. 이는 Panorama 또는 전용 로그 수집기에서 이미 수집한 로그 데이터를 사용하여 사전 정의된 보고서를 생성하므로 보고서 생성 시 리소스 사용률을 줄입니다. 이 설정을 활성화해야 합니다. 그렇지 않으면 Panorama 성능에 영향을 미치고 Panorama가 응답하지 않을 수 있습니다.

최대 5,000개의 방화벽을 관리하려면 Panorama 관리 서버가 다음 최소 요구 사항을 충족해야 합니다.

요구 사항	방화벽 **5,000**개	방화벽 **2,500**개
모델	M-600 M-700 VMware ESXi	지원되는 모든 Panorama 하이퍼바이저. 자세한 내용은 Panorama 모델를 참조하십시오.
Panorama 모드	관리 전용	관리 전용
시스템 디스크	운영 체제 파일, 시스템 로그, 소프트웨어 업데이트 및 콘텐츠 업데이트를 저장하는 데 사용됩니다. • **M-Series** 어플라이언스 — 240GB SSD • **ESXi** — 224GB 시스템 디스크를 224GB로 직접 늘려야 합니다.	• 81GB - 운영 체제 파일 및 시스템 로그를 저장하는 데 사용됩니다. • Panorama 시스템 및 구성 로그를 저장하는 데 사용되는 최소 92GB 용량의 추가 디스크입니다.
CPU	56	32
메모리	256GB	256GB
로그 수집	로컬 로그 수집은 지원되지 않습니다. 로그 수집을 설정하려면 전용 로그 수집기로 Panorama 배포을(를) 참조하십시오.	
로깅 및 보고	미리 정의된 보고서에 **Panorama** 데이터 사용 설정 활성화(**Panorama** > 설정 > 관리 > 로깅 및 보고 설정 > 로그 내보내기 및 보고)	

©2024 Palo Alto Networks, Inc.

디바이스 관리 용량 증가를 위한 Panorama 설치

디바이스 관리 라이선스를 활성화하면 단일 M-600 Panorama™ 관리 서버 또는 단일 Panorama 가상 어플라이언스에서 1,000개 이상의 방화벽을 관리할 수 있습니다.

STEP 1 | 최대 5,000개의 방화벽을 관리할 수 있는 Panorama 디바이스 관리 라이선스를 얻으려면 Palo Alto Networks 영업 담당자에게 문의하십시오.

- M-600 어플라이언스를 배포하는 경우 `PAN-M-600-P-1K` 디바이스 관리 라이선스를 얻으십시오.
- M-700 어플라이언스를 배포하는 경우 `PAN-M-700-P-1` 디바이스 관리 라이선스를 얻으십시오.
- Panorama 가상 어플라이언스를 배포하는 경우 `PAN-PRA-1000` 디바이스 관리 라이선스를 얻으십시오.

STEP 2 | Panorama 관리 서버를 설정합니다.

- (M-600 및 M-700 기기만 해당) M-시리즈 어플라이언스 설정.

또는

- Panorama 가상 어플라이언스 설정.

STEP 3 | ESXi 서버에서 Panorama용 시스템 디스크 늘리기(224GB).

최대 5,000개의 방화벽을 관리하려면 VMware ESXi에 설치된 Panorama 가상 어플라이언스에 224GB 시스템 디스크가 필요합니다. 자세한 내용은 디바이스 관리 용량 요구 사항 증가의 내용을 참조하십시오.

STEP 4 | Panorama가 아직 이 모드에 있지 않은 경우 Panorama 관리 서버를 관리 전용 모드로 변경하십시오.

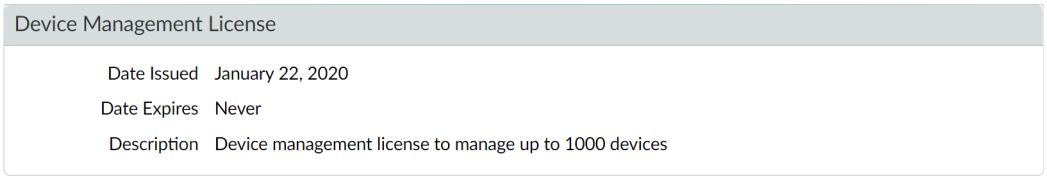
- 5단계~관리 전용 모드에서 M-시리즈 어플라이언스 설정에서 시작합니다.
- 관리 전용 모드에서 Panorama 가상 어플라이언스 설정.

STEP 5 | Panorama 관리 서버를 등록하고 라이선스를 설치합니다.

1. Panorama 등록.
2. Panorama 지원 라이선스 활성화.
3. Panorama 관리 서버에서 디바이스 관리 라이선스를 활성화합니다.
   - M-시리즈 어플라이언스에서 방화벽 관리 라이선스 활성화/검색.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스 활성화/검색.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색.

©2024 Palo Alto Networks, Inc.

STEP 6 | **Panorama** > 라이선스를 선택하고 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.



*Panorama*에서 새 디바이스 관리 라이선스를 활성화하는 경우 *ESXi*에 설치된 *M-600*, *M-700* 어플라이언스 또는 *Panorama* 가상 어플라이언스로 최대 *5,000*개의 방화벽을 관리하거나, *Panorama* 가상 어플라이언스로 최대 *2,500*개의 방화벽을 관리할 수 있지만 *# # 1,000# ### ##### ### # ## #### ## ####*가 설명에 계속 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스 설정

Panorama 가상 어플라이언스를 사용하면 기존 VMware 가상 인프라를 사용하여 Palo Alto Networks 방화벽 및 전용 로그 수집기를 중앙에서 관리하고 모니터링할 수 있습니다. ESXi 서버, Alibaba Cloud, Amazon Web Services(AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform(GCP), KVM, Hyper-V 또는 vCloud Air에 가상 어플라이언스를 설치할 수 있습니다. 전용 로그 수집기s를 배포하는 것 외에 또는 배포하는 대신 Panorama 가상 어플라이언스에 방화벽 로그를 직접 포워딩할 수 있습니다. 더 큰 로그 저장 용량과 더 빠른 보고를 위해 가상 어플라이언스를 레거시 모드에서 Panorama 모드로 전환하고 로컬 로그 수집기를 구성하는 옵션이 있습니다. Panorama 가상 어플라이언스 및 해당 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

이 항목에서는 사용자가 가상 어플라이언스를 생성하는 데 필요한 공용 및 개인 하이퍼바이저 제품에 익숙하다고 가정하고 관련 개념이나 용어를 다루지 않습니다.

- Panorama 가상 어플라이언스의 전제 조건 설정
- Panorama 가상 어플라이언스 설치
- Panorama 가상 어플라이언스의 초기 구성 수행
- Panorama 가상 어플라이언스를 로그 수집기로 설정
- 로컬 로그 수집기로 Panorama 가상 어플라이언스 설정
- Panorama 모드에서 Panorama 가상 어플라이언스 설정
- 관리 전용 모드에서 Panorama 가상 어플라이언스 설정
- Panorama 가상 어플라이언스에서 로그 스토리지 용량 확장
- Panorama 가상 어플라이언스에서 CPU 및 메모리 늘리기
- Panorama 가상 어플라이언스의 시스템 디스크 늘리기
- Panorama 가상 어플라이언스 설정 완료
- Panorama 가상 어플라이언스 변환

Panorama 가상 어플라이언스의 전제 조건 설정

Panorama Virtual Appliance를 설치하기 전에 다음 작업을 완료하십시오.

- 브라우저를 사용하여 Palo Alto Networks 고객 지원 웹 사이트에 액세스하고 Panorama 등록을 선택합니다. 주문 이행 이메일로 받은 Panorama 일련번호가 필요합니다. Panorama를 등록한 후 Panorama 소프트웨어 다운로드 페이지에 액세스할 수 있습니다.
- 지원되는 Panorama 하이퍼바이저를 검토하여 하이퍼바이저가 Panorama 배포를 위한 최소 버전 요구 사항을 충족하는지 확인하십시오.
- VMware ESXi 서버에 Panorama를 설치하는 경우 서버가 Panorama 가상 어플라이언스의 시스템 요구 사항에 나열된 최소 요구 사항을 충족하는지 확인하십시오. 이러한 요구 사항은 Panorama 5.1 이상

©2024 Palo Alto Networks, Inc.

릴리스에 적용됩니다. 요구 사항은 가상 어플라이언스를 Panorama 모드 또는 관리 전용 모드에서 실행할지의 여부에 따라 다릅니다. 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

*VMware vCloud Air*에 *Panorama*를 설치하는 경우 설치 중에 시스템 설정을 지정합니다.

Alibaba Cloud, Amazon Web Services(AWS), AWS GovCloud, Microsoft Azure, Google Cloud Platform(GCP), Hyper-V, KVM, Oracle Cloud Infrastructure(OCI) 및 가상 머신이 원하는 모드(Panorama, 관리 전용 또는 로그 수집기)에 필요한 최소 리소스를 충족하는지 확인하기 위한 VMware ESXi에서 Panorama 가상 어플라이언스를 배포하기 위해 최소 리소스 요구사항을 검토합니다. Panorama 가상 어플라이언스에 대한 최소 리소스 요구 사항은 Panorama 및 Log Collector 모드에서 로그 수집을 위한 최대 LPS(초당 로그 수)를 달성하는 데 도움이 되도록 설계되었습니다. 권장되는 가상 로깅 디스크 수(아래)를 충족하거나 초과하지 않는 구성을 초래하는 가상 로깅 디스크를 추가하거나 제거하면 LPS가 감소합니다.

Panorama 가상 어플라이언스 설치을(를) 할 때, Panorama 모드에 대한 최소 리소스 요구 사항이 충족되지 않으면 Panorama는 지원되는 모든 퍼블릭(Alibaba Cloud, AWS, AWS GovCloud, Azure, GCP 및 OCI) 및 프라이빗(Hyper-V, KVM 및 VMware ESXi) 하이퍼바이저에 대해 오직 관리 모드로만 디폴트합니다. 관리 전용 모드에 대한 최소 리소스 요구 사항이 충족되지 않으면 Panorama는 지원되는 모든 공용 하이퍼바이저, Hyper-V 및 KVM에 대해 기본적으로 유지 관리 모드로 설정됩니다. VMware에 Panorama 설치을(를) 할 때, 관리 전용 모드에 대한 최소 리소스 요구 사항이 충족되지 않으면 Panorama는 기본적으로 레거시 모드로 설정됩니다.

디바이스 관리 및 로그 수집 기능 모두를 위해 *Panorama* 모드에서 *Panorama* 관리 서버를 배포하는 것이 좋습니다. 계속 지원되지만 레거시 모드는 프로덕션 환경에 권장되지 않습니다. 또한 더 이상 *Panorama*를 레거시 모드로 전환할 수 없습니다. 지원되는 모드에 대한 자세한 내용은 Panorama 모델을(를) 참조하십시오.

표 **1: Panorama** 가상 어플라이언스의 시스템 요구 사항

요구 사항	관리 전용 모드의 **Panorama** 가상 어플라이언스	**Panorama** 모드의 **Panorama** 가상 어플라이언스	로그 수집기 모드의 **Panorama** 가상 어플라이언스
가상 하드웨어 버전	• **VMware ESXi** 및 **vCloud Air** — 64비트 커널 기반 VMware ESXi 6.0, 6.5, 6.7, 7.0 또는 8.0. ESXi 서버에서 지원되는 가상 하드웨어 제품군 유형(VMware 가상 하드웨어 버전이라고도 함) 버전은 vmx-10입니다. *ESXi*용 *Panorama* 가상 어플라이언스는 다음을 지원하지 않습니다. • 중지된 스냅샷 생성. 가상 *Panorama* 어플라이언스의 스냅샷을 생성하기 전에 *vSphere* 클라이언트에서 ***Quiesce*** 게스트 파일 시스템을 비활성화하거나 *vSphere CLI*에서 ***quiesce*** 플래그를 *0* 또는 *false*로 설정합니다. • *VMware vMotion*으로 *Panorama* 가상 어플라이언스를 하나의 *ESXi* 서버에서 다른 서버로 마이그레이션.		

 ©2024 Palo Alto Networks, Inc.

요구 사항	관리 전용 모드의 **Panorama** 가상 어플라이언스	**Panorama** 모드의 **Panorama** 가상 어플라이언스	로그 수집기 모드의 **Panorama** 가상 어플라이언스
	• **Hyper-V** — Hyper-V 역할이 있는 Windows Server 2016 또는 Hyper-V 2016/ Hyper-V 역할이 있는 Windows Server 2019 또는 Hyper-V 2019 Hyper-V 역할이 있는 Windows Server 2022 또는 Hyper-V 2022는 지원되지 않습니다. • **KVM**—Ubuntu 버전 16.04 또는 CentOS7 Panorama 모드에서 모든 ESXi 버전에서 실행되는 가상 어플라이언스는 각각 2TB의 로그 스토리지가 있는 최대 12개의 가상 로깅 디스크를 지원하여 총 최대 용량은 24TB입니다. (VMware ESXi 및 vCloud Air만 해당) 레거시 모드에서 가상 디바이스는 하나의 가상 로깅 디스크를 지원합니다. ESXi 5.5 이상의 버전은 최대 8TB의 디스크 하나를 지원합니다. 이전 ESXi 버전은 최대 2TB의 디스크 하나를 지원합니다.		
(ESXi 및 vCloud Air만 해당) 클라이언트 컴퓨터	Panorama 가상 어플라이언스를 설치하고 해당 리소스를 관리하려면 ESXi 서버와 호환되는 VMware vSphere Client 또는 VMware Infrastructure Client를 설치해야 합니다.		
시스템 디스크	• 기본값 - 81GB • (ESXi 및 GCP만 해당) 업그레이드됨 - 224GB SD-WAN에는 업그레이드된 시스템 디스크가 필요합니다. (Panorama 및 로그 수집기 모드) 8개가 넘는 로깅 디스크를 추가한 경우 업그레이드된 시스템 디스크가 필요합니다. 로그 스토리지의 경우 Panorama는 시스템 디스크 또는 NFS 데이터 저장소 대신 가상 로깅 디스크를 사용합니다. Panorama는 처음에 기본 시스템 디스크 크기로 설치해야 하며, 초기 설치 후 필요에 따라 시스템 디스크 크기를 늘릴 수 있습니다.		

©2024 Palo Alto Networks, Inc.

요구 사항	관리 전용 모드의 **Panorama** 가상 어플라이언스	**Panorama** 모드의 **Panorama** 가상 어플라이언스	로그 수집기 모드의 **Panorama** 가상 어플라이언스

CPU, 메모리 및 로깅 디스크	• 최대 500개의 관리 어플라이언스 관리
	  • 16개의 CPU
	  • 64GB 메모리
	  • 로컬 로그 저장소가 지원되지 않습니다.
	• 최대 1,000개의 관리 어플라이언스 관리
	  • 32개의 CPU
	  • 128GB 메모리
	  • 로컬 로그 저장소가 지원되지 않습니다.
	• 1,000개 이상의 방화벽을 관리하려면 디바이스 관리 용량 요구 사항 증가을(를) 참조하십시오.
		지정된 로깅 속도를 달성하려면 아래의 최소 리소스가 필요합니다.
		• 최대 10,000개의 로그/초(LPS):
		  • 16개의 CPU
		  • 64GB 메모리
		  • 4x2TB 로깅 디스크
		  • 최대 500개의 관리 어플라이언스 관리
		• 최대 20,000개의 로그/초(LPS)
		  • 32개의 CPU
		  • 128GB 메모리
		  • 8x2TB 로깅 디스크
		  • 최대 1,000개의 관리 어플라이언스 관리
			지정된 로깅 속도를 달성하려면 아래의 최소 리소스가 필요합니다.
			• 최대 15,000개의 로그/초(LPS)
			  • 16개의 CPU
			  • 64GB 메모리
			  • 4x2TB 로깅 디스크
			• 초당 최대 25,000개의 로그(LPS)
			  • 32개의 CPU
			  • 128GB 메모리
			  • 8x2TB 로깅 디스크

		추가 로깅 디스크를 추가하려면 Panorama 가상 어플라이언스의 첫 번째 로깅 디스크가 2TB여야 합니다. 첫 번째 로깅 디스크가 2TB 미만이면 로깅 디스크를 더 추가할 수 없습니다.	
최소 CPU 및 메모리	• 16개의 CPU • 64GB 메모리	아래의 최소 리소스는 LPS를 고려하지 않으며 Panorama 가상 어플라이언스가 추가된 로깅 디스크 수를 기반으로 작동하는 데만 필요합니다. Palo Alto Networks는 위의 권장 리소스를 참조할 것을 권장합니다. 대규모 Panorama 배포의 경우 Panorama 프로비저닝이 부족할 수 있습니다. 이로 인해 성능이 저하될 수 있으며 관리되는 방화벽 수, 구성 크기, Panorama에 로그인한 관리자 수 및 수집된 로그 양에 따라 Panorama가 응답하지 않을 수 있습니다. • **2TB~8TB** - CPU 16개, 64GB 메모리 • **10TB~24TB** - CPU 16개, 128GB 메모리	
저장 용량	관리 전용 모드의 Panorama는 전용 로그 수	2TB ~ 24TB	2TB ~ 24TB

©2024 Palo Alto Networks, Inc.

요구 사항	관리 전용 모드의 **Panorama** 가상 어플라이언스	**Panorama** 모드의 **Panorama** 가상 어플라이언스	로그 수집기 모드의 **Panorama** 가상 어플라이언스
	집기로 로그를 포워딩해야 합니다.		

지원되는 인터페이스

인터페이스는 디바이스 관리, 로그 수집, 수집기 그룹 통신, 라이선스 및 소프트웨어 업데이트에 사용할 수 있습니다. Panorama 가상 어플라이언스는 최대 6개의 인터페이스(MGT 및 Eth1 - Eth5)를 지원합니다.

표 **2:** 공용 하이퍼바이저에 지원되는 인터페이스

기능	알리바바 클라우드	**Amazon Web Services(AWS)** 및 **AWS GovCloud**		**Microsoft Azure**	구글 클라우드 플랫폼(GCP)	**OCI**
디바이스 관리	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스
디바이스 로그 수집	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스
수집기 그룹 커뮤니케이션	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스
라이선스 및 소프트웨어 업데이트	MGT 인터페이스 전용	MGT 인터페이스 전용	MGT 인터페이스 전용	MGT 인터페이스 전용	MGT 인터페이스 전용	MGT 인터페이스 전용

표 **3:** 프라이빗 하이퍼바이저에 지원되는 인터페이스

기능	**KVM**	하이퍼-**V**	**VMware(ESXi, vCloud Air)**
디바이스 관리	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스
디바이스 로그 수집	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스

©2024 Palo Alto Networks, Inc.

기능	KVM	하이퍼-V	VMware(ESXi, vCloud Air)
수집기 그룹 커뮤니케이션	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스
라이선스 및 소프트웨어 업데이트	지원되는 모든 인터페이스	지원되는 모든 인터페이스	지원되는 모든 인터페이스

Panorama 가상 어플라이언스 설치

설치하기 전에 가상 어플라이언스를 Panorama 모드, 관리 전용 모드, 로그 수집기 모드 또는 레거시 모드(VMware만 해당)에서 실행할지 결정합니다. 각 모드에는 Panorama Virtual Appliance의 설정 전제 조건에 설명된 대로 서로 다른 리소스 요구 사항이 있습니다. 설치를 시작하기 전에 전제 조건을 완료해야 합니다.



가장 좋은 방법은 가상 어플라이언스를 *Panorama* 모드로 설치하여 로그 저장 및 보고서 생성을 최적화하는 것입니다. *Panorama* 및 레거시 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

- VMware에 Panorama 설치
- Alibaba Cloud에서 Panorama 설정
- AWS에 Panorama 설치
- AWS GovCloud에 Panorama 설치
- Azure에 Panorama 설치
- Google Cloud Platform에 Panorama 설치
- KVM에 Panorama 설치
- Hyper-V에 Panorama 설치
- Oracle Cloud Infrastructure(OCI)에서 Panorama 설정

VMware에 Panorama 설치

ESXi 및 vCloud Air VMware 플랫폼에 Panorama 가상 어플라이언스를 설치할 수 있습니다.

- ESXi 서버에 Panorama 설치
- vCloud Air에 Panorama 설치
- Panorama 가상 어플라이언스에서 VMware 도구 지원

ESXi 서버에 Panorama 설치

이 지침에 따라 VMware ESXi 서버에 새 Panorama 가상 어플라이언스를 설치하십시오. 기존 Panorama 가상 어플라이언스로 업그레이드하려면 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치로 건너뛰십시오.

©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 11.1 기본 이미지 OVA(Open Virtual Appliance) 파일을 다운로드합니다.

1. Palo Alto Networks 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택하고 **Panorama** 기본 이미지로 필터링하여 OVA 파일(`Panorama-ESX-11.1.0.ova`)을 다운로드합니다.

STEP 2 | Panorama를 설치합니다.

1. VMware vSphere Client를 실행하고 VMware 서버에 연결합니다.
2. 파일 > **OVF** 템플릿 배포를 선택합니다.
3. Panorama OVA 파일을 찾아 선택한 다음 다음을 클릭합니다.
4. 제품 이름 및 설명이 다운로드한 버전과 일치하는지 확인하고 다음을 클릭합니다.
5. Panorama 가상 어플라이언스를 설명하는 이름을 입력하고 다음을 클릭합니다.
6. Panorama 이미지를 설치할 데이터스토어 위치(시스템 디스크) 를 선택합니다. 지원되는 기본 시스템 디스크 크기는 Panorama 가상 어플라이언스의 전제 조건 설정의 내용을 참조하십시오. 데이터 저장소를 선택한 후 다음을 클릭합니다.

   > *Panorama* 가상 어플라이언스는 처음에 기본 시스템 디스크 크기로 설치되어야 합니다. 기본 시스템 디스크 크기보다 큰 시스템 디스크를 사용하여 *Panorama* 가상 어플라이언스를 설치하는 것은 지원되지 않으며 사용률이 제한될 수 있습니다. 초기 설치 후에 필요에 따라 시스템 디스크 크기를 늘릴 수 있습니다.
7. 디스크 형식으로 **Thick Provision Lazy Zeroed**를 선택한 다음 다음을 클릭합니다.
8. Panorama 가상 어플라이언스에 사용할 인벤토리의 네트워크를 지정하고 다음을 클릭합니다.
9. 선택한 옵션을 확인하고 마침을 클릭하여 설치 프로세스를 시작한 다음 완료되면 닫기를 클릭합니다. 아직 Panorama 가상 어플라이언스의 전원을 켜지 마십시오.

©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama 가상 어플라이언스에서 리소스를 구성합니다.

1. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
2. 하드웨어 설정에서 필요에 따라 CPU와 메모리를 할당하십시오.

   충분한 ***CPU***와 메모리를 할당하고 가상 로깅 디스크를 추가하면 가상 어플라이언스가 *Panorama* 모드로 부팅됩니다*(*이 절차의 뒷부분*)*. 그렇지 않으면 어플라이언스가 관리 전용 모드로 부팅됩니다. 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.
3. **SCSI** 컨트롤러를 **LSI Logic Parallel**로 설정합니다.
4. (선택 사항) 가상 로깅 디스크를 추가합니다.

   이 단계는 다음 시나리오에서 필요합니다.

   - *Panorama* 모드에서 전용 로깅 디스크에 로그를 저장합니다.
   - 관리 전용 모드에서 *SD-WAN* 배포를 관리합니다.

   1. 디스크를 추가하고 하드웨어 유형으로 하드 디스크를 선택한 후 다음을 클릭합니다.

   2. 새 가상 디스크를 생성하고 다음을 클릭합니다.

   3. 디스크 크기를 정확히 2TB로 설정하십시오.

   Panorama 모드에서는 나중에 각각 *2TB*의 저장 공간이 있는 추가 로깅 디스크(총 12개)를 추가할 수 있습니다. *Panorama*에 이미 추가된 로깅 디스크의 크기 확장은 지원되지 않습니다.

   4. 선호하는 디스크 프로비저닝 디스크 형식을 선택하십시오.

   디스크 프로비저닝 형식을 선택할 때 비즈니스 요구 사항을 고려하십시오. 디스크 프로비저닝 성능 고려 사항에 대한 자세한 내용은 VMware Thick vs Thin 디스크와 올 플래시 어레이 문서 또는 추가 VMware 문서를 참조하십시오.

   여러 로깅 디스크를 추가할 때 발생할 수 있는 예기치 않은 성능 문제를 방지하기 위해 모든 디스크에 대해 동일한 디스크 프로비저닝 형식을 선택하는 것이 가장 좋습니다.

   5. 데이터스토어 또는 데이터스토어 구조를 위치로 지정을 선택한 다음 스토리지가 충분한 데이터스토어로 이동한 후 확인을 클릭하고 다음을 클릭합니다.

   6. SCSI 가상 디바이스 노드를 선택한 다음(기본 선택을 사용할 수 있음) 다음을 클릭합니다.

   SCSI 이외의 형식을 선택하면 *Panorama*가 부팅되지 않습니다.

   7. 설정이 올바른지 확인하고 마침을 클릭합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama 가상 어플라이언스의 전원을 켭니다.

1. vSphere Client에서 Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다. 계속하기 전에 Panorama가 부팅될 때까지 기다리십시오.
2. ESXi 콘솔에서 Panorama 가상 어플라이언스 CLI에 로그인합니다.
   1. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 콘솔 열기를 선택합니다.
   2. 사용자 이름과 비밀번호를 입력하여 로그인합니다(기본값은 둘 다 **admin**입니다).

STEP 5 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 장비의 웹 인터페이스 또는 CLI에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. 새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

Panorama CLI에 처음 로그인할 때 계속하려면 먼저 ###의 이전 암호와 새 암호를 입력하라는 메시지가 표시됩니다.

STEP 6 | Panorama가 올바른 시스템 모드로 실행되고 있는지 확인합니다.

```
admin> show system info
```

출력에서 ### ##는 Panorama 또는 ## ## 모드를 나타냅니다.

STEP 7 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.
2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.
3. 방화벽 관리 라이선스를 활성화합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.
4. Panorama 지원 라이선스를 활성화합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 다음에 대해 Panorama 가상 어플라이언스를 사용하려는 경우 ESXi 서버에서 Panorama용 시스템 디스크 늘리기.

- Panorama 모드에서 SD-WAN 배포를 관리합니다.
- 대규모 방화벽 배포를 관리할 때 동적 업데이트를 위한 추가 저장 공간이 필요합니다.

STEP 9 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 ESXi 서버의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     > *Panorama* 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 *IP* 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.
- Panorama 모드의 Panorama용.
  1. ESXi 서버의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.
- SD-WAN 배포용.
  1. ESXi 서버에서 Panorama용 시스템 디스크 늘리기

     ESXi에 배포된 Panorama에서 SD-WAN을 활용하려면 시스템 디스크를 224GB로 늘려야 합니다.

     > 시스템 디스크를 *224GB*로 성공적으로 늘린 후에는 *81GB* 시스템 디스크로 다시 마이그레이션할 수 없습니다.
  2. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  3. ESXi 서버의 Panorama에 가상 디스크 추가.

     SD-WAN을 활용하려면 관리 전용 모드에서 Panorama에 단일 2TB 로깅 디스크를 추가해야 합니다.

©2024 Palo Alto Networks, Inc.

vCloud Air에 Panorama 설치

이 지침에 따라 VMware vCloud Air에 새 Panorama 가상 어플라이언스를 설치하십시오. vCloud Air에 배포된 Panorama 가상 디바이스를 업그레이드하는 경우 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치로 건너뜁니다.

STEP 1 | Panorama 11.1 기본 이미지 OVA(Open Virtual Appliance) 파일을 다운로드합니다.

1. Palo Alto Networks 소프트웨어 다운로드 사이트로 이동합니다. (로그인할 수 없는 경우 Palo Alto Networks 고객 지원 웹사이트로 이동하여 도움을 받으십시오.)
2. Panorama 기본 이미지 섹션의 다운로드 열에서 Panorama 11.1 릴리즈 OVA 파일(`Panorama-ESX-10.0.0.ova`)을 다운로드합니다.

STEP 2 | Panorama 이미지를 vCloud Air 카탈로그로 가져옵니다.

이 단계에 대한 자세한 내용은 OVF Tool 사용자 가이드를 참조하십시오.

1. 클라이언트 시스템에 OVF 도구를 설치합니다.
2. 클라이언트 시스템 CLI에 액세스합니다.
3. OVF Tool 디렉토리(예: C:\Program Files\VMware\VMware OVF Tool)로 이동합니다.
4. OVA 파일을 OVF 패키지로 변환:

```
ovftool.exe <OVA#file#pathname> <OVF#file#pathname>
```

5. 브라우저를 사용하여 vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud OnDemand** 위치를 선택한 다음 브라우저 URL을 기록하십시오. URL 정보를 사용하여 다음 단계를 완료합니다. URL 형식: **`https://<virtual#cloud#location>.vchs.vmware.com/compute/cloud/org/<vCloud#account#number>/#/catalogVAppTemplateList?catalog=<catalog#ID>`**.
6. vCloud Air URL의 정보를 사용하여 OVF 패키지를 가져와서 <virtual-cloud-location>, <vCloud-account-number> 및 <catalog-ID>변수를 작성합니다. 다른 변수는 vCloud Air 사용자 이름 및 도메인 <user>@<domain>, 가상 데이터 센터 <datacenter> 및 vCloud Air 템플릿 <template>입니다.

```
ovftool.exe -st="OVF" "<OVF#file#pathname>"
 "vcloud://<user>@<domain>:password@<virtual-cloud-
location>.vchs.vmware.com?vdc=<datacenter>&org=<vCloud-
account-number>&vappTemplate=<template>.ovf&catalog=default-
catalog"
```


©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama를 설치합니다.

1. vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud OnDemand** 지역을 선택합니다.
2. Panorama 가상 머신을 만듭니다. 단계는 vCloud Air 설명서 센터의 템플릿에서 가상 시스템 추가를 참조하십시오. **CPU**, 메모리 및 스토리지를 다음과 같이 구성합니다.
   - 가상 어플라이언스 모드 여부에 따라 **CPU** 및 메모리를 설정합니다. Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.
   - 스토리지를 설정하여 Panorama 가상 어플라이언스 시스템 디스크를 구성합니다. Panorama 가상 어플라이언스 모드에 따라 지원되는 디스크 크기는 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오. 더 나은 로깅 및 보고 성능을 위해 **SSD** 가속 옵션을 선택하십시오.

     로그 스토리지 용량을 늘리려면 vCloud Air의 Panorama에 가상 디스크를 추가해야 합니다. Panorama 모드에서 가상 어플라이언스는 로그 저장을 위해 시스템 디스크를 사용하지 않습니다. 가상 로깅 디스크를 추가해야 합니다.

STEP 4 | 게이트웨이에서 vCloud Air NAT 규칙을 생성하여 Panorama 가상 디바이스에 대한 인바운드 및 아웃바운드 트래픽을 허용합니다.

자세한 지침은 vCloud Air 설명서 센터에서 NAT 규칙 추가를 참조하십시오.

1. Panorama가 방화벽에서 트래픽을 수신하도록 허용하고 관리자가 Panorama에 액세스하도록 허용하는 NAT 규칙을 추가합니다.
2. Panorama가 Palo Alto Networks 업데이트 서버에서 업데이트를 검색하고 방화벽에 액세스할 수 있도록 하는 NAT 규칙을 추가합니다.

STEP 5 | Panorama 가상 디바이스에서 인바운드 트래픽을 허용하는 vCloud Air 방화벽 규칙을 생성합니다.

아웃바운드 트래픽은 기본적으로 허용됩니다.

자세한 지침은 vCloud Air 설명서 센터에서 방화벽 규칙 추가를 참조하십시오.

STEP 6 | Panorama 가상 어플라이언스가 아직 켜져 있지 않은 경우 전원을 켭니다.

vCloud Air 웹 콘솔에서 가상 머신 탭을 선택한 다음 Panorama 가상 머신을 선택한 다음 전원 켜기를 클릭합니다.

이제 Panorama 가상 어플라이언스의 초기 구성을 수행할 준비가 되었습니다.

Panorama 가상 어플라이언스에서 **VMware** 도구 지원

VMware Tools는 Panorama 가상 어플라이언스용 소프트웨어 이미지(ovf)와 함께 번들로 제공됩니다. VMware 도구 지원을 통해 다음에 대해 vSphere 환경(vCloud Director 및 vCenter 서버)을 사용할 수 있습니다.

- Panorama 관리 인터페이스에 할당된 IP 주소를 봅니다.
- 하드 디스크, 메모리 및 CPU에 대한 리소스 사용률 메트릭을 봅니다. 이러한 메트릭을 사용하여 vCenter 서버 또는 vCloud Director에서 경보 또는 작업을 활성화할 수 있습니다.
- vCenter 서버 또는 vCloud Director의 전원 끄기 기능을 사용하여 Panorama를 정상적으로 종료하고 다시 시작합니다.

 ©2024 Palo Alto Networks, Inc.

- Panorama가 작동하는지 확인하거나 방화벽/Panorama가 재부팅 중인지 확인하기 위해 vCenter 서버와 Panorama 간의 하트비트 메커니즘을 활성화합니다. 방화벽이 유지 관리 모드로 전환되면 vCenter 서버가 방화벽을 종료하지 않도록 하트비트가 비활성화됩니다. 하트비트를 비활성화하면 하트비트를 vCenter 서버로 보낼 수 없을 때 방화벽이 유지 관리 모드에서 작동 상태를 유지할 수 있습니다.

Alibaba Cloud에서 Panorama 설정

물리적 방화벽과 VM 시리즈 방화벽의 구성을 중앙에서 관리하도록 Alibaba Cloud에 Panorama™ 가상 어플라이언스를 설정하십시오.

- Panorama 가상 어플라이언스 이미지를 Alibaba Cloud에 업로드
- Alibaba Cloud에 Panorama 설치

Panorama 가상 어플라이언스 이미지를 Alibaba Cloud에 업로드

KVM용 Panorama™ 관리 서버 qcow2 파일을 업로드하고 Panorama 가상 어플라이언스를 시작하는 데 필요한 사용자 지정 이미지를 생성하려면 다음 절차를 완료하십시오. 이미지 업로드 및 생성은 한 번만 필요합니다. Panorama 가상 어플라이언스의 모든 후속 배포에 동일한 이미지를 사용할 수 있습니다.

STEP 1 | Palo Alto Networks CSP(고객 지원 포털)에서 KVM용 Panorama qcow2 파일을 다운로드합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택한 다음 소프트웨어 업데이트 필터 드롭다운에서 **Panorama** 기본 이미지를 선택합니다.
3. `Panorama-KVM` qcow2 파일의 최신 버전을 다운로드합니다.

STEP 2 | Alibaba Cloud Console에 로그인합니다.

STEP 3 | Panorama 가상 어플라이언스 이미지에 대한 OSS(Object Storage Service) 버킷을 생성합니다.

1. Alibaba Cloud 메뉴에서 개체 스토리지 서비스 > 버킷 및 버킷 생성을 선택합니다.
2. 설명이 포함된 버킷 이름을 입력합니다.
3. 버킷 리전을 선택합니다.

   이 지역은 Panorama 가상 어플라이언스를 배포하려는 지역과 Panorama로 관리하려는 방화벽과 동일한 지역에 있어야 합니다.
4. 필요에 따라 나머지 OSS 버킷 설정을 구성합니다.
5. 확인을 클릭합니다.

   생성에 성공하면 자동으로 OSS 버킷 개요 페이지로 이동합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | qcow2 파일을 OSS 버킷에 업로드합니다.

1. OSS 버킷 개요에서 파일을 선택한 다음 이전 단계에서 다운로드한 qcow2 파일을 업로드합니다.
2. 업로드 대상에 대해 현재를 선택합니다.
3. 파일 **ACL**에 대해 버킷에서 상속됨을 선택합니다.
4. 파일 선택을 클릭하고 qcow2 파일을 선택합니다.

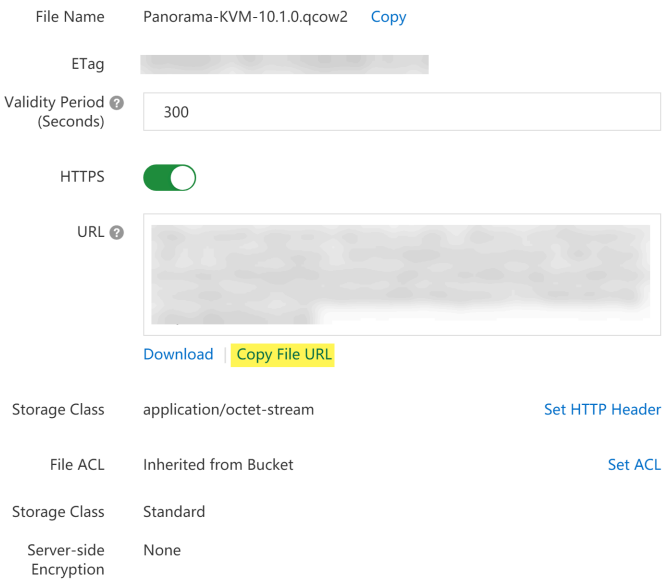
   또는 qcow2 파일을 업로드할 파일 섹션으로 끌어다 놓을 수 있습니다.
5. qcow2 파일을 업로드합니다.

   업로드 상태를 표시하는 작업 목록 창이 나타납니다. qcow2 파일 업로드 상태에 업로드됨이 표시되면 다음 단계로 계속 진행합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | qcow2 파일을 부팅 가능한 이미지로 생성합니다.

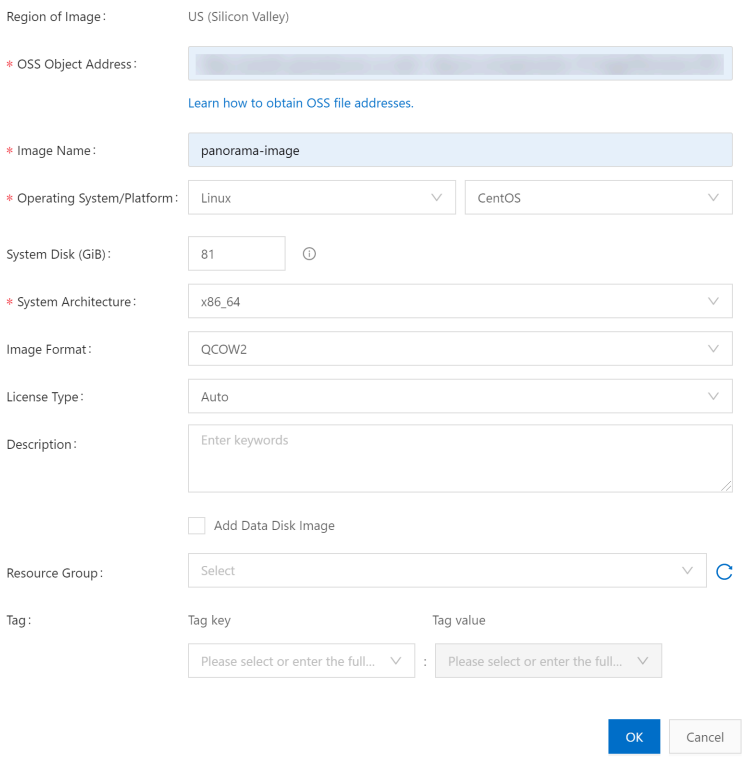
1. OSS 버킷 개요에서 파일을 선택한 다음 업로드한 qcow2 파일을 클릭하여 파일 세부 정보를 봅니다.
2. 파일 **URL** 복사를 클릭하고 파일 세부 정보를 종료합니다.



3. Alibaba Cloud 메뉴에서 **Elastic Compute Service** > 인스턴스 **&** 이미지 > 이미지 및 이미지 가져오기를 선택합니다.
4. qcow2 파일의 **OSS** 개체 주소를 붙여넣습니다.

   이전 단계에서 복사한 파일 URL입니다.
5. 이미지 이름을 입력합니다.
6. 운영 체제/플랫폼의 경우 **Linux CentOS**를 선택합니다.
7. 시스템 디스크**(GiB)**에 **81**을 입력합니다.
8. 시스템 아키텍처의 경우 **x86_64**를 선택합니다.
9. 이미지 형식으로 **QCOW2**를 선택합니다.
10. 확인을 클릭합니다.

©2024 Palo Alto Networks, Inc.



Alibaba Cloud에 **Panorama** 설치

Elastic Compute Service(ECS)를 사용하여 Alibaba Cloud에서 Panorama™ 가상 어플라이언스 인스턴스를 생성하십시오. ECS 인스턴스는 기본적으로 단일 NIC를 지원하며 ENI(탄력적 네트워크 인터페이스)를 자동으로 연결합니다. Alibaba Cloud에 Panorama 가상 어플라이언스를 성공적으로 설치하려면 Palo Alto Networks CSP(고객 지원 포털)에서 다운로드한 Panorama 가상 어플라이언스 qcow2 이미지를 Alibaba Cloud에 수동으로 업로드해야 합니다.

Alibaba Cloud에 배포된 Panorama 가상 어플라이언스는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을(를) 참조하십시오.

Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토하여 필요에 맞는 올바른 ECS(Elastic Computer Service) 인스턴스 유형을 결정하십시오. Panorama 가상 어플라이언스에 대한 가상 리소스 요구 사항은 Panorama 가상 어플라이언스에서 관리하는 총 방화벽 수와 관리되는 방화벽에서 Log Collector로 로그를 포워딩하는 데 필요한 LPS(초당 로그)를 기반으로 합니다.

Palo Alto Networks는 다음 인스턴스 유형을 지원합니다.

- `ecs.g5.xlarge`, `ecs.g5.2xlarge`, `ecs.g5.4xlarge`
- `ecs.sn2ne.xlarge`, `ecs.sn2ne.2xlarge`, `ecs.sn2ne.4xlarge`

Panorama 가상 어플라이언스의 프로비저닝이 부족하면 관리 성능에 영향을 미칩니다. 여기에는 *Panorama* 가상 어플라이언스의 프로비저닝 부족 정도에 따라 *Panorama* 가상 어플라이언스가 느려지거나 응답하지 않는 것이 포함됩니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | Alibaba Cloud Console에 로그인합니다.

STEP 2 | Panorama 가상 어플라이언스 이미지를 Alibaba Cloud에 업로드.

STEP 3 | 네트워크 요구 사항에 맞게 가상 사설 클라우드(VPC)를 설정합니다.

기존 VPC에서 Panorama 가상 어플라이언스를 시작하든 새 VPC를 생성하든 Panorama 가상 어플라이언스는 VPC의 다른 인스턴스에서 트래픽을 수신하고 필요에 따라 VPC와 인터넷 간에 인바운드 및 아웃바운드 통신을 수행할 수 있어야 합니다.

자세한 내용은 Alibaba Cloud VPC 설명서를 참조하십시오.

1. VPC를 생성하고 네트워크를 구성하거나 기존 VPC를 사용합니다.
2. 네트워크 및 보안 구성 요소가 적절하게 정의되었는지 확인합니다.
   - 인터넷 게이트웨이를 생성하여 Panorama 가상 어플라이언스의 서브넷에 대한 인터넷 액세스를 활성화합니다. 소프트웨어 및 콘텐츠 업데이트를 설치하고, 라이선스를 활성화하고, Palo Alto Networks 클라우드 서비스를 활용하려면 인터넷 액세스가 필요합니다. 그렇지 않으면 수동으로 업데이트를 설치하고 라이선스를 활성화해야 합니다.
   - 서브넷을 생성합니다. 서브넷은 Alibaba Cloud 인스턴스를 시작할 수 있는 VPC에 할당된 IP 주소 범위의 세그먼트입니다. 필요한 경우 인터넷에 액세스하도록 구성할 수 있도록 Panorama 가상 어플라이언스가 관리 서브넷에 속하는 것이 좋습니다.
   - 프라이빗 서브넷의 라우팅 테이블에 경로를 추가하여 트래픽이 VPC의 서브넷을 통해 라우팅되고 해당되는 경우 인터넷에서 라우팅될 수 있도록 합니다.

     다음 간의 통신을 허용하려면 서브넷 간에 경로를 생성해야 합니다.

     - Panorama, 관리 방화벽 및 로그 수집기.
     - (선택 사항) Panorama 및 인터넷.
   - VPC가 VPC 트래픽을 관리할 수 있도록 다음 수신 보안 규칙이 허용되는지 확인하십시오. 각 규칙의 수신 트래픽 소스는 배포 토폴로지에 고유합니다.

     자세한 내용은 Panorama에 사용되는 포트를 참조하십시오.

     - SSH(포트 **22**) 트래픽을 허용하여 Panorama CLI에 대한 액세스를 활성화합니다.
     - Panorama 웹 인터페이스에 대한 액세스를 활성화하려면 HTTPS(포트 **443** 및 **27280**) 트래픽을 허용합니다.
     - 포트 **3978**의 트래픽을 허용하여 Panorama 간의 통신을 활성화하고 방화벽을 관리하며 로그 수집기를 관리합니다. 이 포트는 또한 로그 수집기가 Panorama로 로그를 포워딩하는 데 사용됩니다.
     - 포트 **28443**에서 트래픽을 허용하여 관리 방화벽이 Panorama에서 소프트웨어 및 콘텐츠 업데이트를 받을 수 있도록 합니다.

STEP 4 | **Elastic Compute Service** > 인스턴스 **&** 이미지 > 인스턴스를 선택한 다음 오른쪽 상단 모서리에서 인스턴스 생성을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama 가상 어플라이언스 인스턴스를 생성합니다.

1. 사용자 지정 실행을 선택합니다.
2. Panorama 가상 어플라이언스 인스턴스를 구성합니다.
   - 청구 방법 - 인스턴스에 대해 원하는 구독 방법을 선택합니다.
   - 지역 - 원하는 지역을 선택합니다. 선택하는 지역은 지원되는 인스턴스 유형을 제공해야 합니다.
   - 인스턴스 유형 - 지원되는 인스턴스 유형 중 하나를 선택합니다. 유형 기반 선택을 선택하여 인스턴스 유형을 검색할 수 있습니다.
   - 이미지 - 사용자 지정 이미지를 선택한 다음 업로드한 Panorama 가상 어플라이언스 이미지를 선택합니다.
   - 스토리지 - 디스크 유형을 선택한 다음 시스템 디스크 용량으로 **81**GiB를 입력합니다.
   - (선택 사항) 디스크 추가 - 추가 로깅 디스크를 추가합니다.

     Panorama 모드에서 또는 전용 로그 수집기로 Panorama 가상 어플라이언스를 사용하려는 경우 초기 배포 중에 가상 로깅 디스크를 추가하십시오. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드 리소스 요구 사항을 충족하고 하나 이상의 가상 로깅 디스크를 추가한 경우 초기 배포 시 Panorama 모드에 있습니다. 그렇지 않으면 Panorama 가상 어플라이언스는 기본적으로 관리 전용 모드로 설정됩니다. 디바이스 및 전용 로그 수집기를 관리하고 로컬에서 로그를 수집하지 않으려면 Panorama 가상 어플라이언스를 관리 전용 모드로 변경하십시오.

     Alibaba Cloud의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. 2TB보다 작은 로깅 디스크 또는 2TB 로깅 디스크 요구 사항으로 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. Panorama 가상 어플라이언스는 2TB보다 큰 로깅 디스크를 2TB 파티션으로 분할합니다.
   - (선택 사항) 스냅샷 - 위험 및 우발적인 데이터 삭제를 방지하기 위해 Panorama 가상 어플라이언스 인스턴스의 스냅샷이 자동으로 생성되는 빈도를 지정합니다.
   - 기간 - Panorama 가상 어플라이언스 인스턴스의 기간을 지정합니다.

STEP 6 | Panorama 가상 어플라이언스 네트워크 설정을 구성합니다.

1. 다음을 선택합니다. 네트워킹.
2. Panorama 가상 어플라이언스 인스턴스에 대한 네트워크 설정을 구성합니다.
   - 네트워크 유형 - 생성한 VPC 및 관리 VSwitch를 선택합니다.
   - 공용 **IP** 주소 - 공용 IP 주소가 없는 경우 공용 **IPv4** 주소 할당을 활성화(선택)하면 공용 IPv4 주소가 Panorama 가상 어플라이언스 인스턴스에 자동으로 할당됩니다.

     특정 IP 주소 또는 특정 범위의 주소를 사용해야 하는 경우 사용자 지정 IP 주소를 요청할 수 있습니다. 탄력적 IP 주소 사용 설명서를 참조하십시오.
   - 보안 그룹 - 생성한 관리 보안 그룹을 선택한 다음 포트 **443(HTTPS)**, 포트 **22** 및 포트 **3389**를 활성화합니다.
   - 탄력적 네트워크 인터페이스 - 구성이 필요하지 않습니다. 관리 인터페이스는 이미 **eth0**에 연결되어 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 가상 어플라이언스 인스턴스 시스템 설정을 구성합니다.

1. 다음을 선택합니다. 시스템 구성.
2. Panorama 가상 어플라이언스 인스턴스에 대한 시스템 설정을 구성합니다.
   - 로그온 자격 증명 - 키 쌍을 선택한 다음 키 쌍을 선택합니다. 키 페어가 아직 생성되지 않은 경우 키 페어 생성을 선택하여 Alibaba Cloud에서 새 키 페어를 생성하거나 기존 키 페어를 가져옵니다.

     비밀번호 인증은 지원되지 않습니다.

   - 인스턴스 이름 - Panorama 가상 어플라이언스를 설명하는 이름을 입력합니다. Alibaba Cloud Console 전체에서 인스턴스에 대해 표시되는 이름입니다.
   - 호스트 - Panorama 가상 어플라이언스 인스턴스의 호스트 이름을 입력합니다.

STEP 8 | (선택 사항) 다음을 선택합니다. **Panorama** 가상 어플라이언스 인스턴스와 연결된 모든 **Alibaba Cloud** 리소스에 대한 그룹화 구성에 대한 그룹화.

STEP 9 | 주문하기 전에 구성을 보려면 미리보기를 선택하십시오.

STEP 10 | **ECS** 서비스 약관 및 제품 서비스 약관을 보고 확인하십시오.

STEP 11 | 인스턴스를 생성하여 Panorama 가상 어플라이언스 인스턴스를 생성합니다.

메시지가 표시되면 콘솔을 클릭하여 인스턴스 생성 상태를 확인합니다.

STEP 12 | 탄력적 IP(EIP) 주소를 할당합니다.

EIP는 Panorama 가상 어플라이언스에 연결하는 데 사용되는 공용 IP 주소입니다.

이 단계는 Panorama 가상 어플라이언스에 대한 인터넷 액세스를 활성화하려는 경우에만 필요합니다.

1. **Elastic Compute Service** > 네트워크 및 보안 > **VPC** > 탄력적 **IP** 주소 > 탄력적 **IP** 주소를 선택합니다.

   기존 EIP가 없는 경우 **EIP** 생성을 선택합니다.
2. 작업 열에서 리소스 바인딩을 선택하여 EIP를 인터넷에 노출된 인터페이스에 바인딩합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | SSH를 사용해 Panorama CLI에 로그인을(를) 수행하여 Panorama 가상 어플라이언스 네트워크 설정을 구성합니다.

암호, 시스템 IP 주소, 넷마스크 및 기본 게이트웨이를 구성해야 합니다. 또한 Palo Alto Networks 업데이트 서버에 성공적으로 연결하려면 Alibaba Cloud DNS 서버를 추가해야 합니다.



Alibaba 콘솔에서 *Panorama CLI*에 액세스할 수도 있습니다. *Alibaba* 콘솔에서 *Panorama CLI*에 액세스하려면 ***Elastic Compute Service*** > 인스턴스 ***&*** 이미지 > 인스턴스를 선택한 다음 *Panorama* 가상 어플라이언스 인스턴스를 선택합니다. 인스턴스 세부 정보에서 연결을 선택합니다.

*Alibaba VCN*에서 처음 연결할 때 *Panorama* 가상 어플라이언스 인스턴스에 대한 *VCN* 암호를 생성하라는 메시지가 표시됩니다. 이 암호는 복구할 수 없으며 나중에 *VCN*을 사용하여 연결하거나 암호를 업데이트해야 하므로 반드시 저장하십시오.

STEP 14 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 어플라이언스의 웹 인터페이스 또는 CLI에 액세스하려면 고유한 관리 암호를 구성해야 합니다. CLI에 액세스하려면 Panorama 가상 어플라이언스를 실행하는 데 사용되는 개인 키가 필요합니다.

새 비밀번호는 최소 8자 이상이어야 하며 최소 소문자 1개, 대문자 1개, 숫자 또는 특수 문자 1개 이상을 포함해야 합니다.

다음 명령을 사용하여 새 암호를 구성하고 화면의 지시를 따릅니다. 명령:

```
admin> configure admin# set mgt-config users admin password
```


©2024 Palo Alto Networks, Inc.

STEP 15 | Panorama 가상 어플라이언스의 초기 네트워크 설정을 구성합니다.

```
admin> configure
```

```
admin#  set deviceconfig system type static
```

```
admin#  set deviceconfig system ip-address <instance-private-IP
 address> netmask <netmask> default-gateway <default-gateway-IP>
```

*Alibaba Cloud*의 기본 게이트웨이는 ***.253***으로 끝납니다. 예를 들어 *Panorama* 가상 어플라이언스 인스턴스의 프라이빗 *IP* 주소가 *192.168.100.20*인 경우 기본 게이트웨이는 *192.168.100.253*입니다.

```
admin#  set deviceconfig system dns-setting servers primary
 100.100.2.136
```

```
admin#  set deviceconfig system dns-setting servers secondary
 100.100.2.138
```

```
admin# ##
```

STEP 16 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

©2024 Palo Alto Networks, Inc.

STEP 17 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- (관리 전용 모드) 관리 전용 모드에서 Panorama 가상 어플라이언스 설정.
- (로그 수집기 모드) Panorama 모드에서 로그 수집기 모드로 전환하려면 6단계부터 시작합니다.

  Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 *IP* 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.
- (Panorama 및 관리 전용 모드) 관리형 수집기 구성 전용 로그 수집기를 Panorama 가상 어플라이언스에 추가합니다. 관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

STEP 18 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 Alibaba Cloud의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 *IP* 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.
- Panorama 모드의 Panorama용.
  1. 필요에 따라 Alibaba Cloud의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

AWS에 Panorama 설치

이제 Amazon Web Services(AWS)에 Panorama™ 및 전용 로그 수집기를 배포할 수 있습니다. AWS에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | AWS Web Service 콘솔에 로그인하고 EC2 대시보드를 선택합니다.

- Amazon Web Service Console
- AWS GovCloud 웹 서비스 콘솔

STEP 2 | 네트워크 요구 사항에 맞게 가상 사설 클라우드(VPC)를 설정합니다.

기존 VPC에서 Panorama 가상 어플라이언스를 시작하든 새 VPC를 생성하든 Panorama 가상 어플라이언스는 VPC의 다른 인스턴스에서 트래픽을 수신하고 필요에 따라 VPC와 인터넷 간에 인바운드 및 아웃바운드 통신을 수행할 수 있어야 합니다.

VPC 생성 및 액세스 설정에 대한 지침은 AWS VPC 설명서를 참조하십시오.

1. 새 VPC를 생성하거나 기존 VPC를 사용합니다. AWS 시작하기 설명서 참조
2. 네트워크 및 보안 구성 요소가 적절하게 정의되었는지 확인합니다.
   - 인터넷 게이트웨이를 생성하여 Panorama 가상 어플라이언스의 서브넷에 대한 인터넷 액세스를 활성화합니다. 소프트웨어 및 콘텐츠 업데이트를 설치하고, 라이선스를 활성화하고, Palo Alto Networks 클라우드 서비스를 활용하려면 인터넷 액세스가 필요합니다. 그렇지 않으면 수동으로 업데이트를 설치하고 라이선스를 활성화해야 합니다.
   - 서브넷을 생성합니다. 서브넷은 AWS 인스턴스를 시작할 수 있는 VPC에 할당된 IP 주소 범위의 세그먼트입니다. 필요한 경우 인터넷에 액세스하도록 구성할 수 있도록 Panorama 가상 어플라이언스가 관리 서브넷에 속하는 것이 좋습니다.
   - 프라이빗 서브넷의 라우팅 테이블에 경로를 추가하여 트래픽이 VPC의 서브넷을 통해 라우팅되고 해당되는 경우 인터넷에서 라우팅될 수 있도록 합니다.

     다음 간의 통신을 허용하려면 서브넷 간에 경로를 생성해야 합니다.

     - Panorama, 관리 방화벽 및 로그 수집기.
     - (선택 사항) Panorama 및 인터넷.
   - VPC가 VPC 트래픽을 관리할 수 있도록 다음 인바운드 보안 규칙이 허용되는지 확인하십시오. 각 규칙의 수신 트래픽 소스는 배포 토폴로지에 고유합니다.

     자세한 내용은 Panorama에 사용되는 포트를 참조하십시오.

     - SSH(포트 **22**) 트래픽을 허용하여 Panorama CLI에 대한 액세스를 활성화합니다.
     - Panorama 웹 인터페이스에 대한 액세스를 활성화하려면 HTTPS(포트 **443**) 트래픽을 허용합니다.
     - 포트 **3978**의 트래픽을 허용하여 Panorama 간의 통신을 활성화하고 방화벽을 관리하며 로그 수집기를 관리합니다. 이 포트는 또한 로그 수집기가 Panorama로 로그를 포워딩하는 데 사용됩니다.
     - 포트 **28443**에서 트래픽을 허용하여 관리 방화벽이 Panorama에서 소프트웨어 및 콘텐츠 업데이트를 받을 수 있도록 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Amazon Web Services에 Panorama를 배포합니다.

1. 서비스 > **EC2** > 인스턴스 및 인스턴스 시작을 선택합니다.
2. **AWS Marketplace**를 선택하고 **`Palo Alto Networks Panorama`**를 검색한 후 Panorama AMI를 선택하고 계속하십시오.
3. Panorama 가상 어플라이언스에 필요한 리소스를 할당하기 위한 **EC2** 인스턴스 유형을 선택한 다음 다음을 클릭합니다. 인스턴스 세부 정보를 구성합니다. 리소스 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

   Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 초기 배포 중에 필요한 리소스로 어플라이언스를 구성해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하는 경우 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

4. 인스턴스 세부 정보를 구성합니다.
   1. 다음을 선택합니다. 인스턴스 세부 정보를 구성합니다.
   2. 네트워크에서 VPC를 선택합니다.
   3. 서브넷을 선택합니다.
   4. 공용 **IP**를 자동 할당하려면 사용을 선택합니다.

      이 IP는 Panorama를 사용하여 관리하려는 방화벽에서 액세스할 수 있어야 합니다. 이를 통해 Panorama 가상 어플라이언스의 관리 인터페이스에 대해 공개적으로 액세스할 수 있는 IP 주소를 얻을 수 있습니다. 나중에 탄력적 IP 주소를 관리 인터페이스에 연결할 수 있습니다. 인스턴스가 종료될 때 가상 어플라이언스에서 연결 해제된 공용 IP 주소와 달리 탄력적 IP 주소는 지속성을 제공하며 IP 주소를 재구성할 필요 없이 Panorama 가상 어플라이언스의 새(또는 교체) 인스턴스에 IP 주소를 할당할 수 있습니다. Panorama 가상 어플라이언스 인스턴스의 전원이 꺼질 때마다 주소를 지정합니다.
   5. 필요에 따라 추가 인스턴스 세부 정보를 구성합니다.
5. (선택 사항) Panorama 가상 장비 스토리지를 구성합니다.
   1. 다음을 선택합니다. 스토리지를 추가합니다.
   2. 추가 로그 스토리지를 추가하려면 새 볼륨을 추가하십시오.

      (SD-WAN만 해당) 관리 전용 모드에서 SD-WAN 배포를 관리하려는 경우 2TB 로깅 디스크를 추가해야 합니다.

      Panorama 모드에서 또는 전용 로그 수집기로 Panorama 가상 어플라이언스를 사용하려는 경우 초기 배포 중에 가상 로깅 디스크를 추가하십시오. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드 리소스 요구 사항을 충족하고 하나 이상의 가상 로깅 디스크를 추가한 경우 초기 배포 시 Panorama 모드에 있습니다. 그렇지 않으면 Panorama 가상 어플라이언스는 기본적으로 관리 전용 모드로 설정됩니다. 디바이스 및 전용 로그 수집기를 관리하고 로컬에서 로그를 수집하지 않으려면 Panorama 가상 어플라이언스를 관리 전용 모드로 변경하십시오.

      AWS의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. 2TB보다 작은 로깅 디스크 또는 2TB 로깅 디스크 요구 사항으로 나눌

 ©2024 Palo Alto Networks, Inc.

수 없는 크기의 로깅 디스크를 추가할 수 없습니다. Panorama 가상 어플라이언스는 2TB보다 큰 로깅 디스크를 2TB 파티션으로 분할합니다.

6. (선택 사항) 다음을 선택합니다. 태그를 추가하고 하나 이상의 태그를 메타데이터로 추가하면 Panorama 가상 어플라이언스를 식별하고 그룹화하는 데 도움이 됩니다. 예를 들어 Panorama 가상 어플라이언스가 관리하는 방화벽을 식별하는 데 도움이 되는 값이 포함된 이름 태그를 추가합니다.
7. 인스턴스 보안 그룹을 구성합니다.
   1. 다음을 선택합니다. 보안 그룹을 구성합니다.
   2. Panorama 가상 어플라이언스 인스턴스에 대한 보안 그룹을 할당할 기존 보안 그룹을 선택합니다.
   3. 이전에 생성한 보안 그룹을 선택합니다.

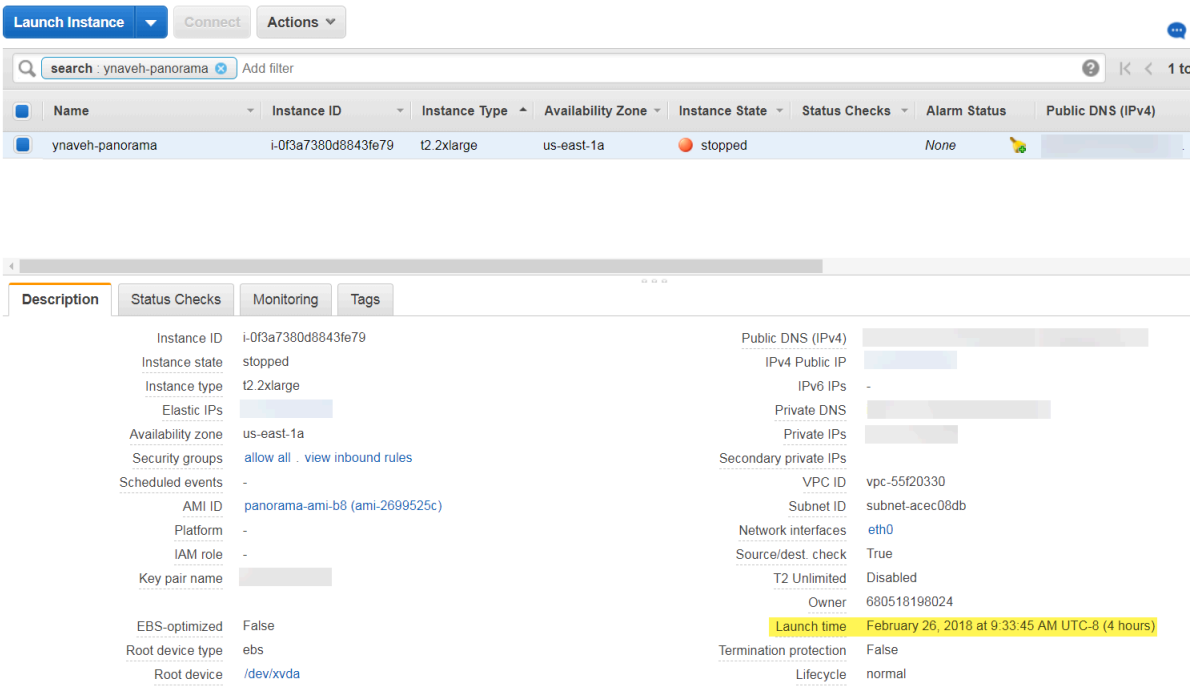
      모든 인바운드 및 아웃바운드 트래픽 유형을 허용하도록 ## 보안 그룹을 선택할 수 있습니다.
8. Panorama 가상 어플라이언스 인스턴스를 검토하고 시작하여 시작하기 전에 선택 사항이 정확한지 확인하십시오.
9. 기존 키 쌍을 선택하거나 새 키 쌍을 생성하고 고지 사항을 확인합니다.

   *AWS*에서 새 키를 생성한 경우 키를 다운로드하여 안전한 위치에 저장합니다. 파일 확장자는 *.pem*입니다. 공개 키를 PuTTYgen에 로드하고 *.ppk* 형식으로 저장해야 합니다. 이 키를 분실하면 다시 생성할 수 없습니다.

AWS에서 Panorama 가상 어플라이언스를 시작한 후 배포를 완료하는 데 약 30분이 걸립니다. Panorama 가상 어플라이언스 배포는 인스턴스에 연결된 디스크의 수와 크기에 따라 더 오래 걸

 ©2024 Palo Alto Networks, Inc.

릴 수 있습니다. Panorama 가상 어플라이언스 인스턴스(인스턴스)를 선택하여 시작 시간을 봅니다.



Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 필요한 리소스로 어플라이언스를 프로비저닝해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하면 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

STEP 4 | Panorama 가상 어플라이언스를 종료합니다.

1. EC2 대시보드에서 인스턴스를 선택합니다.
2. Panorama 가상 어플라이언스를 선택한 다음인스턴스 상태 > 인스턴스 중지를 클릭합니다.

STEP 5 | 탄력적 IP(EIP) 주소를 생성하거나 관리 인터페이스에 할당합니다.

1. 서비스 > **EC2** > 탄력적 **IP** 및 탄력적 **IP** 주소 할당을 선택합니다.
2. 네트워크 경계 그룹을 선택하여 공용 IP4v 주소가 보급되는 논리적 영역 그룹을 지정합니다.
3. 퍼블릭 IPv4 주소 풀에서 **Amazon**의 **IPv4** 주소 풀을 선택합니다.
4. EIP를 할당합니다.
5. 할당된 IPv4 주소 열에서 IPv4 주소를 클릭하고 탄력적 **IP** 주소 연결을 클릭합니다.
6. Panorama 가상 어플라이언스 인스턴스를 선택합니다.
7. EIP를 연결할 Panorama 가상 어플라이언스 사설 **IP** 주소를 선택합니다.

STEP 6 | Panorama 가상 어플라이언스의 전원을 켭니다.

1. EC2 대시보드에서 인스턴스를 선택합니다.
2. 목록에서 Panorama 가상 어플라이언스를 선택한 다음 작업 > 인스턴스 상태 > 시작을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 어플라이언스의 웹 인터페이스에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. CLI에 액세스하려면 Panorama 가상 어플라이언스를 시작하는 데 사용되는 개인 키가 필요합니다.

새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

- 컴퓨터에 SSH 서비스가 설치되어 있는 경우:
  1. 다음 명령을 입력하여 Panorama 가상 어플라이언스에 로그인합니다.

     ```
     ssh -i <private_key.ppk> admin@<public-ip_address>
     ```

  2. 다음 명령을 사용하여 새 암호를 구성하고 화면의 지시를 따릅니다.

     ```
     admin> configure admin# set mgt-config users admin password
     ```

  3. BYOL을 활성화해야 하는 경우 Panorama 가상 어플라이언스가 Palo Alto Networks 라이선스 서버에 액세스할 수 있도록 DNS 서버 IP 주소를 설정하십시오. 다음 명령을 입력하여 DNS 서버 IP 주소를 설정합니다.

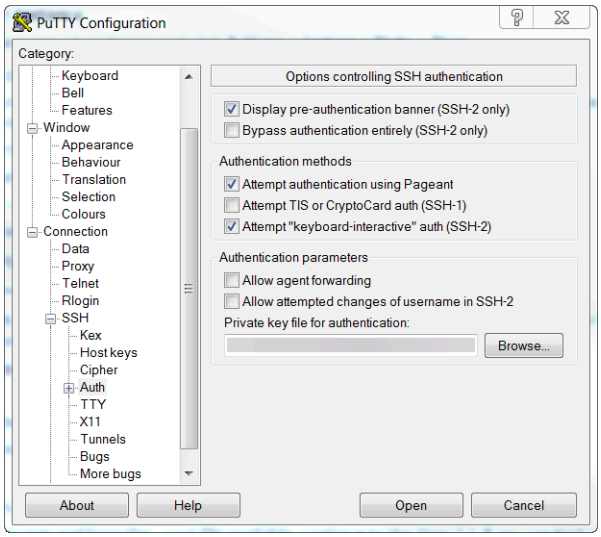
     ```
     admin# set deviceconfig system dns-setting servers
      primary <ip_address>
     ```

  4. 다음 명령을 사용하여 변경 사항을 커밋합니다.

     ```
     admin# commit
     ```

  5. SSH 세션을 종료합니다.
- PuTTY를 사용하여 Panorama 가상 어플라이언스에 SSH로 연결하는 경우:
  1. 기존 키 쌍을 사용 중이고 `.ppk` 파일을 사용할 수 있는 경우 7.3단계로 계속 진행합니다. 새 키 쌍을 생성했거나 기존 키 쌍의 `.pem` 파일만 있는 경우 PuTTYgen을 열고 `.pem` 파일을 로드합니다.
  2. 개인 키를 액세스 가능한 로컬 대상에 저장합니다.
  3. PuTTY를 열고 **SSH** > **Auth**를 선택한 다음 이전 단계에서 저장한 `.ppk` 파일을 찾습니다.

©2024 Palo Alto Networks, Inc.



4. 세션을 선택한 다음 Panorama 가상 어플라이언스의 공용 IP 주소를 입력합니다. 열기를 클릭하고 보안 프롬프트가 나타나면 예를 클릭합니다.
5. 메시지가 표시되면 관리자로 로그인합니다.
6. 다음 명령을 사용하여 새 암호를 구성하고 화면의 지시를 따릅니다.

```
admin> configure admin# set mgt-config users admin password
```

7. Panorama 가상 어플라이언스가 Palo Alto Networks 라이선스 서버에 액세스할 수 있도록 DNS 서버 IP 주소를 설정합니다. 다음 명령을 입력하여 DNS 서버 IP 주소를 설정합니다.

```
admin# set deviceconfig system dns-setting servers
 primary <ip_address>
```

8. 다음 명령을 사용하여 변경 사항을 커밋합니다.

```
admin# commit
```

9. SSH 세션을 종료합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

STEP 9 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 AWS의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 ***IP*** 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.

- Panorama 모드의 Panorama용.
  1. AWS의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

©2024 Palo Alto Networks, Inc.

AWS GovCloud에 Panorama 설치

이제 Amazon Web Services(AWS) GovCloud에 Panorama™ 및 전용 로그 수집기를 배포할 수 있습니다. AWS GovCloud는 미국 정부 기관 및 고객의 규정 및 규정 준수 요구 사항을 충족하는 격리된 AWS 리전입니다. AWS GovCloud에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, 로그 수집기 및 관리 전용)를 지원합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을(를) 참조하십시오.

AWS GovCloud(US) 리전에서 모든 카테고리의 CUI(Controlled Unclassified Information) 데이터와 정부 지향의 공개적으로 사용 가능한 데이터를 포함하는 워크로드를 보호하기 위해 Panorama 가상 어플라이언스는 AWS GovCloud의 표준 AWS 퍼블릭 클라우드에서 제공하는 것과 동일한 보안 기능을 제공합니다. AWS GovCloud의 Panorama 가상 어플라이언스와 표준 AWS 퍼블릭 클라우드는 동일한 기능을 지원합니다.

지원되는 EC2 인스턴스 유형을 검토하려면 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토하십시오. 준비가 되면 AWS에 Panorama 설치을(를) 참조하여 AWS GovCloud에 Panorama 가상 어플라이언스 설치하십시오.

Panorama 가상 어플라이언스에 로깅 스토리지를 추가하거나 할당된 CPU 코어 및 메모리를 늘리려면 다음 절차를 참조하십시오.

- AWS의 Panorama에 가상 디스크 추가
- Panorama on AWS의 CPU 및 메모리 증가

Azure에 Panorama 설치

이제 Microsoft Azure에 Panorama™ 및 전용 로그 수집기를 배포할 수 있습니다. Azure에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, 로그 수집기 및 관리 전용)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

STEP 1 | Microsoft Azure 포털에 로그인합니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | 네트워크 요구 사항에 맞게 가상 네트워크를 설정합니다.

기존 가상 네트워크에서 Panorama 가상 어플라이언스를 시작하든 새 가상 네트워크를 생성하든 Panorama 가상 어플라이언스는 가상 네트워크의 다른 인스턴스에서 트래픽을 수신하고 필요에 따라 가상 네트워크와 인터넷 간에 인바운드 및 아웃바운드 통신을 수행할 수 있어야 합니다.

자세한 내용은 Microsft Azure Virtual Network 설명서를 참조하세요.

1. 가상 네트워크를 만들거나 기존 가상 네트워크를 사용합니다.
2. 네트워크 및 보안 구성 요소가 적절하게 정의되었는지 확인합니다.
   - Panorama 가상 어플라이언스가 속한 서브넷에 대해 아웃바운드 인터넷 액세스만 활성화하려면 NAT 게이트웨이를 생성합니다.
   - 서브넷을 생성합니다. 서브넷은 Microsoft Azure 인스턴스를 시작할 수 있는 VNet에 할당된 IP 주소 범위의 일부분입니다. 필요한 경우 인터넷에 액세스하도록 구성할 수 있도록 Panorama 가상 어플라이언스가 관리 서브넷에 속하는 것이 좋습니다.
   - 프라이빗 서브넷의 라우팅 테이블에 경로를 추가하여 VNet의 서브넷과 해당되는 경우 인터넷에서 트래픽을 라우팅할 수 있도록 합니다.

     다음 간의 통신을 허용하려면 서브넷 간에 경로를 생성해야 합니다.

     - Panorama, 관리 방화벽 및 로그 수집기.
     - (선택 사항) Panorama 및 인터넷.
   - VNet이 VNet 트래픽을 관리할 수 있도록 다음 수신 보안 규칙이 허용되는지 확인합니다. 각 규칙의 수신 트래픽 소스는 배포 토폴로지에 고유합니다.

     자세한 내용은 Panorama에 사용되는 포트를 참조하십시오.

     - SSH(포트 **22**) 트래픽을 허용하여 Panorama CLI에 대한 액세스를 활성화합니다.
     - Panorama 웹 인터페이스에 대한 액세스를 활성화하려면 HTTPS(포트 **443**) 트래픽을 허용합니다.
     - 포트 **3978**의 트래픽을 허용하여 Panorama 간의 통신을 활성화하고 방화벽을 관리하며 로그 수집기를 관리합니다. 이 포트는 또한 로그 수집기가 Panorama로 로그를 포워딩하는 데 사용됩니다.
     - 포트 **28443**에서 트래픽을 허용하여 관리 방화벽이 Panorama에서 소프트웨어 및 콘텐츠 업데이트를 받을 수 있도록 합니다.

STEP 3 | Panorama 가상 어플라이언스를 배포합니다.

1. Azure 대시보드에서 가상 머신 및 새 가상 머신 추가를 선택합니다.
2. Palo Alto Networks를 검색하고 최신 Panorama 가상 어플라이언스 이미지를 선택합니다.
3. Panorama 가상 어플라이언스를 생성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama 가상 어플라이언스를 구성합니다.

1. Azure 구독을 선택합니다.
2. 모든 Azure 인스턴스 리소스를 포함할 Azure 리소스 그룹을 선택합니다.
3. Panorama 가상 어플라이언스의 가상 머신 이름을 입력합니다.
4. Panorama 가상 어플라이언스를 배포할 지역을 선택합니다.
5. (선택 사항) 가용성 옵션을 선택합니다. 자세한 내용은 가용성 집합을 사용하는 방법을 참조하십시오.
6. Panorama 관리 서버를 배포하는 데 사용되는 이미지를 선택합니다. Azure Marketplace의 Panorama 이미지에서 Panorama 관리 서버를 배포하려면 모든 공용 및 개인 이미지를 찾습니다.
7. Panorama 가상 어플라이언스 크기를 구성합니다. 크기 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

   Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 초기 배포 중에 필요한 리소스로 어플라이언스를 구성해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하는 경우 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.
8. 고유한 Panorama 가상 어플라이언스 관리자 자격 증명을 구성합니다.

   Panorama 가상 어플라이언스의 웹 인터페이스 및 CLI에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다.

   1. Panorama 가상 어플라이언스 관리자의 사용자 이름을 입력합니다. 사용자 이름이 안전한지 확인하기 위해 admin은 유효한 항목이 아닙니다.
   2. Panorama 가상 어플라이언스에 대한 관리 액세스를 보호하기 위해 암호를 입력하거나 **SSH** 공개 키를 복사하여 붙여넣습니다.

      FIPS-CC 작동 모드에서 *Panorama* 가상 어플라이언스의 이 인스턴스를 사용하려면 *SSH* 키 인증을 활성화해야 합니다. 사용자 이름과 암호를 사용하여 *Panorama* 가상 어플라이언스를 배포할 수 있지만 작동 모드를 *FIPS-CC*로 변경한 후에는 사용자 이름과 암호를 사용하여 인증할 수 없습니다. *FIPS-CC* 모드로 재설정한 후에는 *SSH* 키를 사용하여 로그인해야 하며 이후에 *Panorama* 웹 인터페이스에 로그인하는 데 사용할 수 있는 사용자 이름과 암호를 구성할 수 있습니다. *SSH* 키 생성에 대한 자세한 내용은 Azure 설명서를 참조하세요.
9. Panorama 가상 어플라이언스 인스턴스 네트워킹 구성

   1. 기존 가상 네트워크를 선택하거나 새 가상 네트워크를 생성합니다.
   2. 서브넷을 구성합니다. 서브넷은 이전 단계에서 선택하거나 만든 가상 네트워크에 따라 다릅니다. 기존 가상 네트워크를 선택한 경우 선택한 가상 네트워크의 서브넷 중 하나를 선택할 수 있습니다.
   3. 기존 공용 **IP** 주소를 선택하거나 새 주소를 만드십시오. 그러면 Panorama 가상 어플라이언스에 액세스하는 데 사용되는 관리 인터페이스가 생성됩니다.
   4. 기존 **NIC** 네트워크 보안 그룹을 선택하거나 새 보안 그룹을 생성합니다. 네트워크 보안 그룹은 가상 머신에 대한 트래픽을 제어합니다. 인바운드 규칙에 대해 HTTPS 및 SSH가 허용되는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

10. 인스턴스 관리 설정을 구성합니다.
    1. 자동 종료 활성화 여부를 선택합니다. 자동 종료를 사용하면 가상 머신에 새 공용 IP 주소가 할당되거나 로그가 삭제되거나 로그가 할당되지 않거나 Panorama 가상 어플라이언스가 종료되는 동안에는 방화벽을 관리할 수 없습니다.
    2. 부팅 모니터링 활성화 여부를 선택합니다. 활성화된 경우 진단 저장소 계정을 선택합니다. 모니터링은 부팅 진단 로그를 진단 저장소 계정으로 자동으로 보냅니다. 자세한 내용은 Microsoft Azure의 모니터링 개요를 참조하세요.
    3. 필요에 따라 다른 설정을 구성합니다.
11. 요약을 검토하고 사용 약관 및 개인 정보 보호 정책에 동의하고 Panorama 가상 어플라이언스를 생성합니다.

STEP 5 | Panorama 가상 어플라이언스가 성공적으로 배포되었는지 확인합니다.

1. 대시보드 > 리소스 그룹을 선택한 다음 Panorama 가상 어플라이언스가 포함된 리소스 그룹을 선택합니다.
2. 설정에서 가상 머신 배포 상태에 대해 배포를 선택합니다.

Panorama 가상 어플라이언스를 배포하는 데 약 *30*분이 걸립니다. *Panorama* 가상 어플라이언스 실행은 가상 머신에 대해 구성된 리소스에 따라 더 오래 걸릴 수 있습니다. *Microsoft Azure*는 *ICMP* 프로토콜이 성공적으로 배포되었는지 테스트하는 것을 허용하지 않습니다.

Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 어플라이언스에 필요한 리소스를 올바르게 구성했는지 확인하십시오. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하면 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

STEP 6 | 고정 공용 IP 주소를 구성합니다.

1. Azure Portal에서 가상 머신을 선택한 다음 Panorama 가상 머신을 선택합니다.
2. 개요를 선택한 다음 공용 **IP** 주소를 클릭합니다.
3. 할당에서 고정을 선택한 다음 새 IP 주소 구성을 저장합니다.

STEP 7 | Panorama 가상 어플라이언스의 웹 인터페이스에 로그인합니다.

1. Azure Portal의 모든 리소스에서 Panorama 가상 어플라이언스를 선택한 다음 개요 섹션에 있는 공용 IP 주소를 확인합니다.
2. 웹 브라우저에서 보안(https) 연결을 사용하여 공용 IP 주소를 사용하여 Panorama 가상 어플라이언스에 로그인합니다.
3. Panorama 가상 어플라이언스의 사용자 이름과 암호를 입력합니다. 인증서 경고가 표시됩니다. 인증서 경고를 수락하고 웹 페이지를 계속 진행합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

STEP 9 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 Azure의 Panorama에 가상 디스크를 추가합니다.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 ***IP*** 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.

- Panorama 모드의 Panorama용.
  1. Azure의 Panorama에 가상 디스크를 추가합니다.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

©2024 Palo Alto Networks, Inc.

Google Cloud Platform에 Panorama 설치

이제 Google Cloud Platform(GCP)에 Panorama™ 및 전용 로그 수집기를 배포할 수 있습니다. GCP에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

GCP에 Panorama 가상 어플라이언스를 배포하려면 커스텀 이미지를 빌드해야 합니다. 이 프로세스를 시작하려면 Palo Alto Networks 고객 지원 포털에서 Panorama `tar.gz`를 다운로드하고 GCP 스토리지 버킷에 업로드해야 합니다. 그런 다음 커스텀 이미지를 생성하고 이 이미지를 사용하여 GCP에 Panorama 가상 어플라이언스를 배포할 수 있습니다.

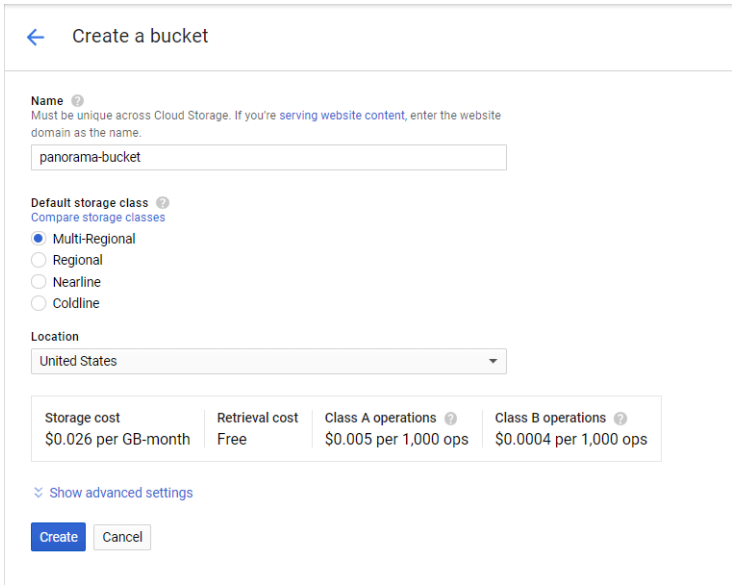
STEP 1 | Panorama 가상 어플라이언스 이미지를 다운로드합니다.

1. Palo Alto Networks 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택하고 **Panorama** 기본 이미지로 필터링합니다.
3. Panorama on GCP `tar.gz` 이미지의 최신 버전을 다운로드합니다.

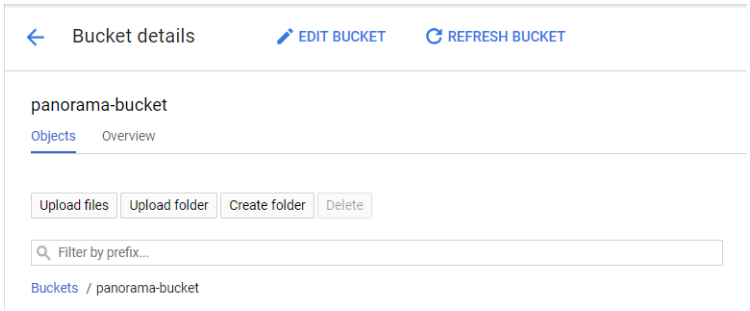
©2024 Palo Alto Networks, Inc.

STEP 2 | Google Cloud Platform에 Panorama 가상 어플라이언스 이미지를 업로드합니다.

1. Google Cloud Console에 로그인합니다.
2. 제품 및 서비스 메뉴에서 스토리지를 선택합니다.
3. 버킷 생성을 클릭하고 새 스토리지 버킷을 구성한 다음 생성을 클릭합니다.

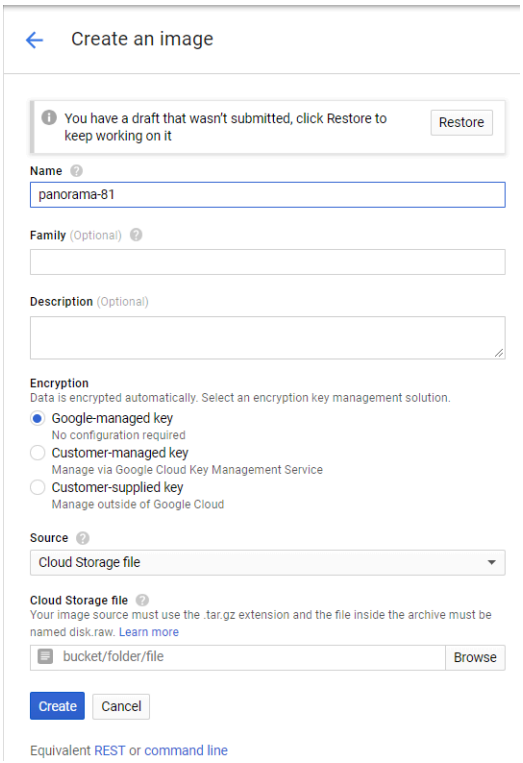


4. 이전 단계에서 생성한 스토리지 버킷을 선택한 다음 파일 업로드를 클릭한 다음 다운로드한 Panorama 가상 어플라이언스 이미지를 선택합니다.



5. 제품 및 서비스 메뉴에서 **Compute Engine** > 이미지를 선택합니다.
6. 이미지 생성을 클릭하고 Panorama 가상 어플라이언스 이미지를 생성합니다.
   1. Panorama 가상 어플라이언스 이미지의 이름을 지정합니다.
   2. 소스 필드의 드롭다운 메뉴에서 **Cloud Storage** 파일을 선택합니다.
   3. 찾아보기를 클릭하고 Panorama 가상 어플라이언스 이미지를 업로드한 스토리지 버킷으로 이동한 다음 업로드된 이미지를 선택합니다.
   4. Panorama 가상 어플라이언스 이미지를 생성합니다.

©2024 Palo Alto Networks, Inc.



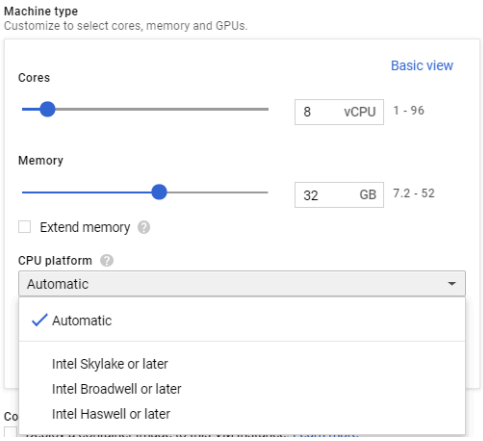
 ©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama 가상 어플라이언스를 구성합니다.

1. 제품 및 서비스 메뉴에서 **Compute Engine**을 선택합니다.
2. 인스턴스 생성을 클릭하여 Panorama 가상 어플라이언스 배포를 시작합니다.
3. Panorama 가상 어플라이언스를 쉽게 식별할 수 있도록 설명이 포함된 이름을 추가합니다.
4. Panorama 가상 어플라이언스를 배포할 지역 및 영역을 선택합니다.
5. 머신 유형을 할당하고 CPU 코어, 메모리 및 CPU 플랫폼을 사용자 정의합니다. 최소 리소스 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

   Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 초기 배포 중에 필요한 리소스로 어플라이언스를 구성해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하는 경우 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

   GCP 영역 선택에 따라 사용 가능한 *CPU* 플랫폼이 결정됩니다. 자세한 내용은 지역 및 영역을 참조하십시오.

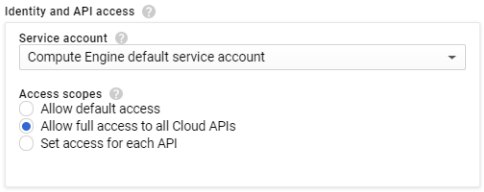


6. Panorama 부팅 디스크를 구성합니다.
   1. **Boot Disk**의 경우 **Change** > **Custom image**를 클릭하고 2단계에서 업로드한 Panorama 이미지 파일을 선택합니다.
   2. 부팅 디스크 크기를 검토하고 시스템 디스크가 **81**GB인지 확인합니다.

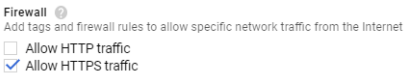
      Panorama 가상 어플라이언스는 처음에 기본 시스템 디스크 크기로 설치되어야 합니다. 기본 시스템 디스크 크기보다 큰 시스템 디스크를 사용하여 *Panorama* 가상 어플라이언스를 설치하는 것은 지원되지 않으며 사용률이 제한될 수 있습니다. 초기 설치 후에 필요에 따라 시스템 디스크 크기를 늘릴 수 있습니다.

   3. 선택을 클릭하여 구성을 저장합니다.
7. **ID** 및 **API** 액세스에서 모든 **Cloud API**에 대한 전체 액세스 허용을 선택합니다.

 ©2024 Palo Alto Networks, Inc.



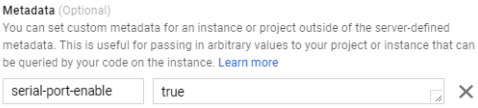
8. 방화벽에서 **HTTPS** 트래픽 허용을 선택합니다.



STEP 4 | 관리, 보안, 디스크, 네트워킹, 단독 임대 Management, security, disks, networking, sole tenancy 를 확장합니다.

STEP 5 | Panorama 가상 어플라이언스를 관리할 수 있도록 직렬 포트에 대한 액세스를 활성화합니다.

1. 관리를 선택합니다.
2. 다음 이름-값 쌍을 메타데이터로 입력하십시오.
   ## ## ### ##(true)



 ©2024 Palo Alto Networks, Inc.

STEP 6 | 관리 인터페이스에 대한 고정 IP 주소를 예약합니다.

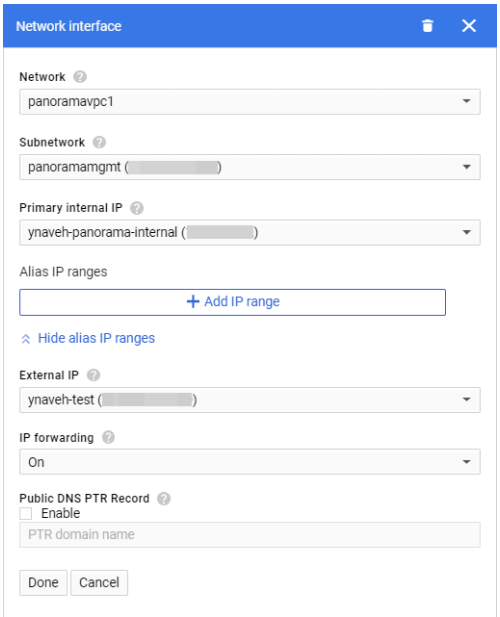
Panorama 가상 어플라이언스가 재부팅되는 경우 IP 주소가 재할당될 때 관리되는 디바이스와 Panorama 가상 어플라이언스의 연결이 끊어지지 않는 경우 관리 인터페이스에 대해 고정 내부 및 외부 IP 주소를 예약하십시오.

IP 주소 예약 방법에 대한 자세한 내용은 고정 내부 IP 주소 예약 및 고정 외부 IP 주소 예약을 참조하세요.

1. 네트워킹을 선택합니다.
2. 네트워크 인터페이스를 편집합니다.



3. Panorama 가상 어플라이언스 네트워크를 선택합니다.
4. Panorama 가상 어플라이언스 서브 네트워크를 선택합니다. 동일한 하위 네트워크의 인스턴스는 내부 IP 주소를 사용하여 서로 통신합니다.
5. 기본 내부 **IP** 주소를 설정합니다.
   - 임시(자동) - 기본 내부 IP 주소를 자동으로 할당합니다.
   - 임시(커스텀) - GCP가 기본 내부 IP 주소를 할당하는 데 사용하는 커스텀 IP 범위를 구성합니다.
   - 고정 내부 **IP** 주소 예약 - 고정 기본 내부 IP 주소를 수동으로 구성합니다.
6. 외부 **IP** 주소를 설정합니다.
   - 임시 - 공유 IP 풀에서 외부 IP 주소를 자동으로 할당합니다.
   - 기존에 예약된 외부 IP 주소를 선택합니다.
   - **IP** 주소 생성 - 외부 IP 주소를 예약합니다.
7. Panorama 가상 어플라이언스가 일치하지 않는 대상 또는 소스 IP 주소에서 패킷을 수신할 수 있도록 **IP** 포워딩을 켜기로 설정합니다.

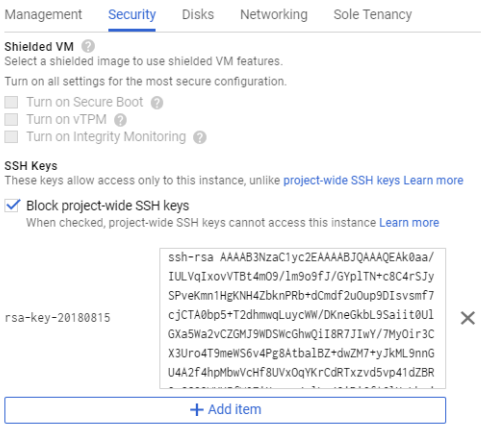


 ©2024 Palo Alto Networks, Inc.

STEP 7 | SSH 키를 구성합니다. 초기 배포 후 관리자 암호를 구성하기 위해 Panorama 가상 어플라이언스 CLI에 액세스하려면 SSH 키가 필요합니다.

- **PuTTY** 사용자
  1. 보안을 선택합니다.
  2. 프로젝트 전체 **SSH** 키 차단 상자를 선택합니다. 초기 배포 후 Panorama 가상 어플라이언스에 로그인할 때 현재 인스턴스 키만 지원됩니다.
  3. 주석 상자에 SSH 키를 붙여넣습니다. 올바른 SSH 키 형식 및 GCP용 SSH 키 생성 방법에 대한 정보는 메타데이터에서 SSH 키 관리를 참조하십시오.

     SSH 키 생성 시 개인 키를 *.ppk* 형식으로 저장합니다. 관리 암호를 구성하기 전에 초기 배포 후 *Panorama* 가상 어플라이언스에 로그인하려면 개인 키가 필요합니다.



- **Linux** 및 **macOS** 사용자
  1. Linux 디바이스의 CLI에서 SSH 키를 생성합니다.

     ```
     ssh-keygen -C admin@panorama -f <panorama_key_name>
     ```

     여기서 **admin@panorama**는 GCP에 필요한 주석이고 **<panorama_key_name>**은(는) 생성되는 키 파일의 이름입니다.
  2. SSH 키에 대한 출력 파일을 생성합니다.

     ```
     cat <panorama_key_name>.pub
     ```

     SSH 키에 대한 출력 파일이 생성된 후 SSH 키 내용을 수동으로 복사합니다.
  3. 공개 키를 GCP 인스턴스 생성의 SSH 키 섹션에 붙여넣습니다.

STEP 8 | (선택 사항) 로그 수집을 위한 추가 저장소를 추가합니다. 가상 로깅 디스크를 추가하려면 필요에 따라 이 단계를 반복합니다.

Panorama 모드에서 또는 전용 로그 수집기로 Panorama 가상 어플라이언스를 사용하려는 경우 초기 배포 중에 가상 로깅 디스크를 추가하십시오. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드 리소스 요구 사항을 충족하고 하나 이상의 가상 로깅 디스크를 추가한 경우 초기 배포

©2024 Palo Alto Networks, Inc.

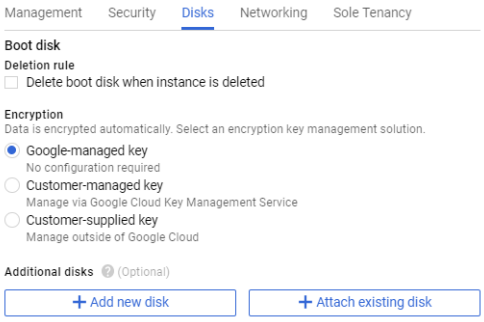
시 Panorama 모드에 있습니다. 그렇지 않으면 Panorama 가상 어플라이언스는 기본적으로 디바이스 및 전용 로그 수집기를 관리할 수 있고 로컬에서 로그를 수집할 수 없는 관리 전용 모드로 설정됩니다.

GCP의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. 2TB보다 작은 로깅 디스크 또는 2TB 로깅 디스크 요구 사항으로 나눌 수 없는 크기의 로깅

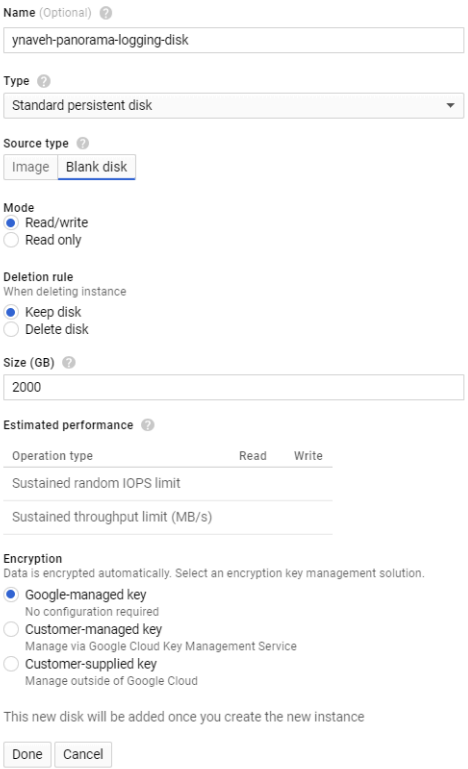
 ©2024 Palo Alto Networks, Inc.

디스크를 추가할 수 없습니다. Panorama 가상 어플라이언스는 2TB보다 큰 로깅 디스크를 2TB 파티션으로 분할합니다.

1. 디스크 > 새 디스크 추가를 선택합니다.



2. 이름을 입력합니다.
3. 유형 드롭다운 메뉴를 확장하고 원하는 유형을 선택합니다.
4. 소스 유형으로 빈 디스크를 선택합니다.
5. 모드에서 읽기/쓰기를 선택합니다.
6. 삭제 규칙을 선택하여 Panorama 가상 어플라이언스 인스턴스가 삭제된 경우 가상 로깅 디스크를 삭제할지의 여부를 구성합니다. 수신지
7. 가상 로깅 디스크의 크기**(GB)**를 설정합니다.
8. 가상 로깅 디스크의 데이터에 대해 선호하는 암호화 솔루션을 설정합니다.
9. 완료를 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 9 | Panorama 가상 어플라이언스를 생성합니다. Panorama 가상 어플라이언스는 초기 배포 후 부팅하는 데 약 10분이 걸립니다.

©2024 Palo Alto Networks, Inc.

STEP 10 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 어플라이언스의 웹 인터페이스에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. CLI에 액세스하려면 개인 키를 사용하여 Panorama 가상 어플라이언스를 시작하십시오.

새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

- 컴퓨터에 SSH 서비스가 설치되어 있는 경우:
  1. 다음 명령을 입력하여 Panorama 가상 어플라이언스에 로그인합니다.
     - Windows 디바이스

       ```
       ssh -i <private_key.ppk> <### ##>@<public-ip_address>
       ```

     - 리눅스 디바이스

       ```
       ssh -i <prive_key.ppk> -oHostKeyAlgorithms=+ssh-rsa <### ##>
        @<public-ip_address>
       ```

       호스트 키 유형을 지정하려면 *-oHostKeyAlgorithms=+ssh-rsa*를 포함해야 합니다. SSH login 명령에 포함되지 않은 경우 오류가 표시됩니다.
  2. 다음 명령을 사용하여 새 암호를 구성하고 화면의 지시를 따릅니다.

     ```
     admin> configure admin# set mgt-config users admin password
     ```

  3. 필요한 BYOL이 있는 경우 Panorama 가상 어플라이언스가 Palo Alto Networks 라이선스 서버에 액세스할 수 있도록 DNS 서버 IP 주소를 설정하십시오. 다음 명령을 입력하여 DNS 서버 IP 주소를 설정합니다.

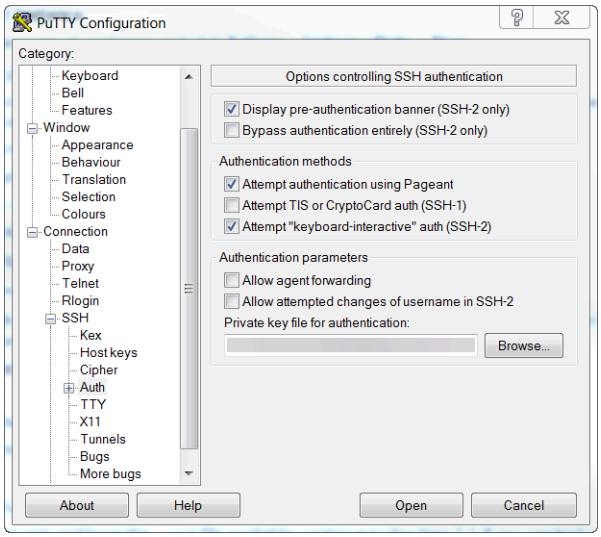
     ```
     admin# set deviceconfig system dns-setting servers
      primary <ip_address>
     ```

  4. 변경 사항을 커밋합니다.

     ```
     admin# commit
     ```

  5. SSH 세션을 종료합니다.
- PuTTY를 사용하여 Panorama 가상 어플라이언스에 SSH로 연결하는 경우:
  1. 기존 키 쌍을 사용 중이고 `.ppk` 파일을 사용할 수 있는 경우 11.3단계로 계속 진행합니다. 새 키 쌍을 생성했거나 기존 키 쌍의 `.pem`파일만 있는 경우 PuTTYgen을 열고 `.pem` 파일을 로드합니다.
  2. 개인 키를 액세스 가능한 로컬 대상에 저장합니다.
  3. PuTTY를 열고 **SSH** > **Auth**를 선택한 다음 이전 단계에서 저장한 `.ppk` 파일에 대해 찾아보기를 선택합니다.

 ©2024 Palo Alto Networks, Inc.



4. 세션을 선택한 다음 Panorama 가상 어플라이언스의 공용 IP 주소를 입력합니다. 그런 다음 열기를 누르고 보안 프롬프트가 나타나면 예를 클릭합니다.
5. 메시지가 표시되면 관리자로 로그인합니다.
6. 다음 명령을 사용하여 새 암호를 구성하고 화면의 지시를 따릅니다.

```
admin> configure admin# set mgt-config users admin password
```

7. Panorama 가상 어플라이언스가 Palo Alto Networks 라이선스 서버에 액세스할 수 있도록 DNS 서버 IP 주소를 설정합니다. 다음 명령을 입력하여 DNS 서버 IP 주소를 설정합니다.

```
admin# set deviceconfig system dns-setting servers
 primary <ip_address>
```

8. 다음 명령을 사용하여 변경 사항을 커밋합니다.

```
admin# commit
```

9. SSH 세션을 종료합니다.

©2024 Palo Alto Networks, Inc.

STEP 11 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

©2024 Palo Alto Networks, Inc.

STEP 12 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 Google Cloud Platform의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 *IP* 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.
- Panorama 모드의 Panorama용.
  1. Google Cloud Platform의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.
- SD-WAN 배포용.
  1. Google Cloud Platform에서 Panorama용 시스템 디스크 늘리기

     GCP에 배포된 Panorama에서 SD-WAN을 활용하려면 시스템 디스크를 224GB로 늘려야 합니다.

     시스템 디스크를 *224GB*로 성공적으로 늘린 후에는 *81GB* 시스템 디스크로 다시 마이그레이션할 수 없습니다.
  2. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  3. Google Cloud Platform의 Panorama에 가상 디스크 추가.

     SD-WAN을 활용하려면 관리 전용 모드에서 Panorama에 단일 2TB 로깅 디스크를 추가해야 합니다.

KVM에 Panorama 설치

이제 Panorama™ 및 전용 로그 수집기를 KVM에 배포할 수 있습니다. KVM에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오.

©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 11.1 기본 이미지 QCOW2 파일을 다운로드합니다.

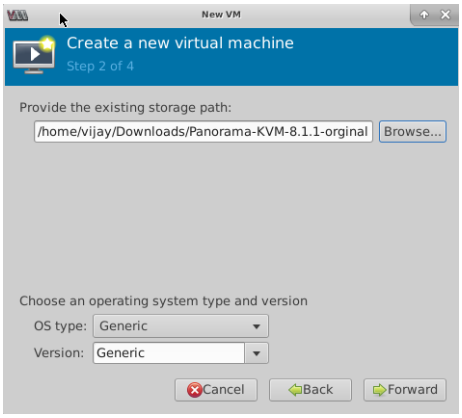
1. Palo Alto Networks 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택하고 **Panorama** 기본 이미지로 필터링한 다음 QCOW2 파일(`Panorama-KVM-11.1.0.qcow2`)을 다운로드합니다.

STEP 2 | 새 가상 머신 이미지를 생성하고 KVM용 Panorama 가상 어플라이언스 이미지를 Virtual Machine Manager에 추가합니다.

1. Virtual Machine Manager에서 새 가상 머신 생성을 선택합니다.
2. 기존 디스크 이미지 가져오기를 선택한 다음 포워드를 클릭합니다.



3. Panorama 가상 어플라이언스 이미지 볼륨을 찾아 선택한 다음 볼륨을 선택합니다.
4. 포워드를 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

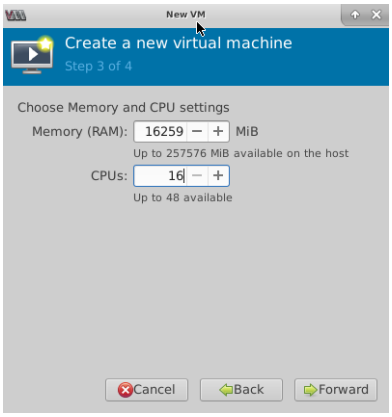
STEP 3 | 메모리 및 CPU 설정을 구성합니다.

최소 리소스 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 초기 배포 중에 필요한 리소스로 어플라이언스를 구성해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하는 경우 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

1. 원하는 작동 모드에 대한 요구 사항에 따라 메모리를 구성합니다.

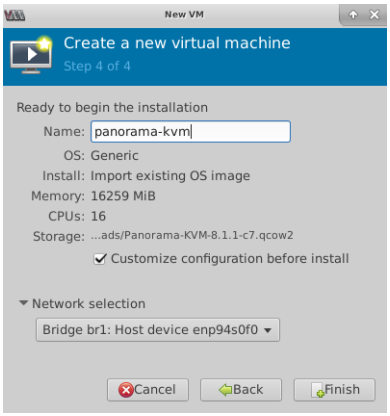
   *Virtual Machine Manager*는 실행 중인 버전에 따라 *MiB*(메비바이트)를 사용하여 메모리를 할당할 수 있습니다. *MiB*를 사용하는 경우 *Panorama* 가상 어플라이언스의 프로비저닝 부족을 방지하기 위해 필요한 메모리 할당을 올바르게 변환해야 합니다.
2. 원하는 작동 모드에 대한 요구 사항에 따라 **CPU**를 구성합니다.
3. 포워드를 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

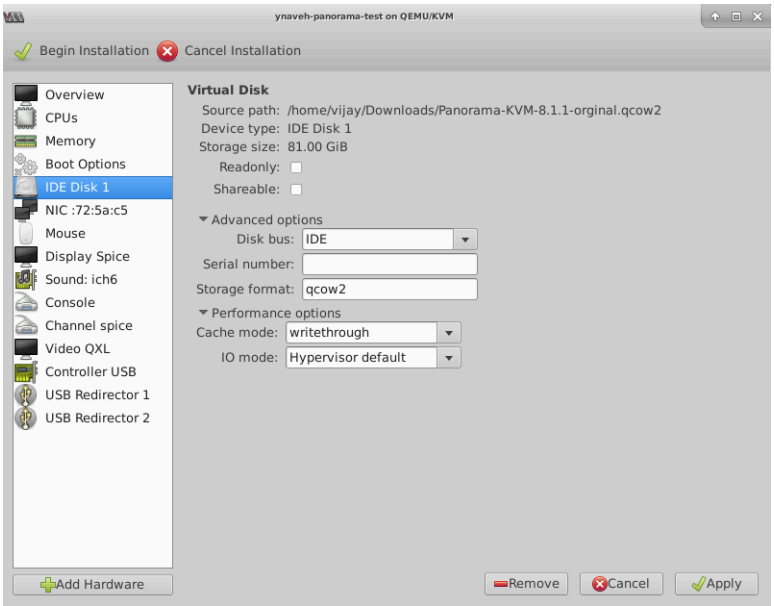
STEP 4 | Panorama 가상 어플라이언스의 이름을 지정하고 구성 사용자 지정을 활성화하고 관리 인터페이스 브리지를 선택합니다.

1. Panorama 가상 어플라이언스를 설명하는 이름을 입력합니다.
2. 설치하기 전에 구성을 사용자 정의하십시오.
3. 네트워크 선택 - 관리 인터페이스에 대한 브리지를 선택한 다음 기본 설정을 수락합니다.
4. 마침을 클릭합니다.



STEP 5 | 가상 시스템 디스크 설정을 구성합니다.

1. **IDE** 디스크 **1**을 선택한 다음 고급 옵션으로 이동하여 다음을 선택합니다.
   - 디스크 버스 - 구성에 따라 **VirtIO** 또는 **IDE**.
   - 저장 형식 - **qcow2**
2. 성능 옵션으로 이동하여 캐시 모드를 연속 기입으로 설정합니다. 이 설정은 Panorama 가상 어플라이언스의 설치 시간과 실행 속도를 향상시킵니다.
3. 적용을 클릭합니다.



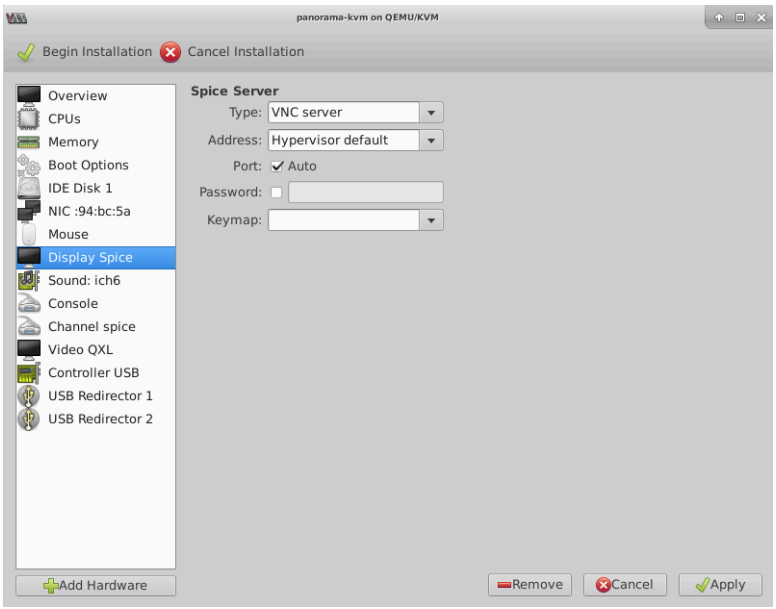
 ©2024 Palo Alto Networks, Inc.

STEP 6 | VNC 서버를 사용하여 가상 머신과 상호 작용하도록 가상 머신 콘솔 디스플레이를 구성합니다.

1. 디스플레이 스파이스를 선택합니다.

   가상 머신이 디스플레이에 *VNC* 서버를 사용하도록 이미 구성되어 있으므로 디스플레이 ***VNC***가 하드웨어 목록에 나열되면 다음 단계를 계속합니다.

2. 유형 드롭다운에서 **VNC** 서버를 선택합니다.
3. 적용을 클릭합니다.



STEP 7 | (선택 사항) 로그 수집을 위한 추가 저장소를 추가합니다. 가상 로깅 디스크를 추가하려면 필요에 따라 이 단계를 반복합니다.

Panorama 모드에서 또는 전용 로그 수집기로 Panorama 가상 어플라이언스를 사용하려는 경우 초기 배포 중에 가상 로깅 디스크를 추가하십시오. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드 리소스 요구 사항을 충족하고 하나 이상의 가상 로깅 디스크를 추가한 경우 초기 배포 시 Panorama 모드에 있습니다. 그렇지 않으면 Panorama 가상 어플라이언스는 기본적으로 관리 전용 모드로 설정됩니다. 디바이스 및 전용 로그 수집기를 관리하고 로컬에서 로그를 수집하지 않으려면 Panorama 가상 어플라이언스를 관리 전용 모드로 변경하십시오.

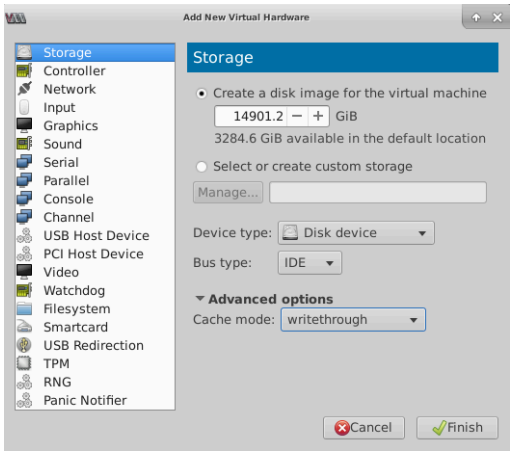
KVM의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. 2TB보다 작은 로깅 디스크 또는 2TB 로깅 디스크 요구 사항으로 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. Panorama 가상 어플라이언스는 2TB보다 큰 로깅 디스크를 2TB 파티션으로 분할합니다.

1. 하드웨어를 추가합니다.

©2024 Palo Alto Networks, Inc.

2. 새 스토리지 디스크를 구성합니다.
   1. 가상 머신에 대한 디스크 이미지를 생성하고 가상 디스크 스토리지 용량을 14901.2GiB(2TB에 해당)로 구성합니다.

      *Virtual Machine Manager*는 실행 중인 버전에 따라 *GiB*(기비바이트)를 사용하여 메모리를 할당할 수 있습니다. *GiB*를 사용하는 경우 가상 로깅 디스크를 프로비저닝하지 않고 *Panorama* 가상 어플라이언스를 유지 관리 모드로 보내는 것을 방지하기 위해 필요한 스토리지 용량을 올바르게 변환해야 합니다.
   2. 디바이스 유형을 디스크 디바이스로 설정합니다.
   3. 구성에 따라 버스 유형을 **VirtIO** 또는 **IDE**로 설정합니다.
   4. **Advanced** 옵션으로 이동하여 캐시 모드를 연속 기입으로 설정합니다.
3. 마침을 클릭합니다.



STEP 8 | 설치를 시작합니다(Begin Installation). Panorama 가상 어플라이언스는 부팅하는 데 약 10분이 걸립니다.

STEP 9 | Panorama 가상 어플라이언스의 콘솔에 대한 연결을 엽니다.

기본 사용자 이름과 암호인 **admin/admin**을 사용하여 방화벽에 로그인합니다.

STEP 10 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 장비의 웹 인터페이스 또는 CLI에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. 새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

Panorama CLI에 처음 로그인할 때 계속하려면 먼저 ###의 이전 암호와 새 암호를 입력하라는 메시지가 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | 관리 인터페이스에 대한 네트워크 액세스 설정을 구성합니다.

1. 다음 명령을 사용하여 구성 모드로 들어갑니다.

```
admin> configure
```

2. 다음 명령을 사용하여 관리 인터페이스에 대한 액세스를 구성하고 활성화합니다.

```
admin# set deviceconfig system type static admin# set
 deviceconfig system ip-address <Panorama-IP>
 netmask <netmask> default-gateway <gateway-IP> dns-setting
 servers primary <DNS-IP>
```

여기서 *<Panorama-IP>*은(는) 관리 인터페이스에 할당하려는 IP 주소, *<netmask>*은(는) 서브넷 마스크, *<gateway-IP>*은(는) 네트워크 게이트웨이의 IP 주소, *<DNS-IP>*은(는) DNS 서버의 IP 주소입니다.

```
admin# commit
```

STEP 12 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 KVM의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 ***IP*** 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.
- Panorama 모드의 Panorama용.
  1. KVM의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.
  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

Hyper-V에 Panorama 설치

이제 Hyper-V에서 Panorama™ 및 전용 로그 수집기를 배포할 수 있습니다. Hyper-V에 배포된 Panorama는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을 참조하십시오. Hyper-V의 Panorama 가상 어플라이언스 및 가상 전용 로그 수집기는 PAN-OS 8.1.3 이상 버전에서만 사용할 수 있습니다.

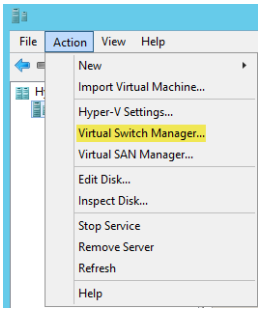
STEP 1 | Panorama 11.1 기본 이미지 VHDX 파일을 다운로드합니다.

1. Palo Alto Networks 지원 포털에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택하고 **Panorama** 기본 이미지로 필터링한 다음 VHDX 파일(`Panorama-HPV-11.1.0.vhdx`)을 다운로드합니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | 필요한 vSwitch를 설정합니다. 자세한 내용은 가상 스위치 유형을 검토하십시오.

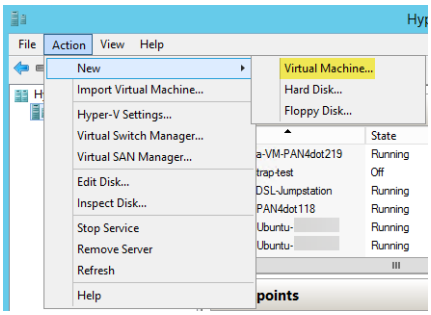
1. Hyper-V 관리자에서 호스트를 선택한 다음 작업 > **Virtual** 스위치 관리자를 선택하여 가상 스위치 관리자 창을 엽니다.



2. 가상 스위치 생성에서 생성할 vSwitch 유형을 선택한 다음 가상 스위치 생성을 클릭합니다.

STEP 3 | Panorama 가상 어플라이언스를 설치합니다.

1. Hyper-V 관리자에서 호스트를 선택한 다음 작업 > 신규 > 가상 머신을 선택합니다. 새 가상 머신 마법사에서 다음 설정을 구성합니다.



1. Panorama 가상 어플라이언스의 이름과 위치를 선택합니다. Panorama 가상 어플라이언스는 VHDX 파일을 지정된 위치에 저장합니다.
2. **1**세대를 선택합니다. 이것은 기본 옵션이며 지원되는 유일한 버전입니다.
3. 시작 메모리의 경우 의도한 시스템 모드에 따라 메모리를 할당합니다. 각 모드의 메모리 요구 사항은 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.

   동적 메모리를 활성화하지 마십시오. *Panorama* 가상 어플라이언스에는 정적 메모리 할당이 필요합니다.
4. 네트워킹을 구성합니다. 방화벽에서 관리 인터페이스를 연결할 외부 vSwitch를 선택합니다.
5. 가상 하드 디스크를 연결하려면 기존 가상 하드 디스크 사용을 선택한 다음 이전에 다운로드한 VHDX 파일을 찾습니다.
6. 요약을 검토하고 마침을 클릭합니다.

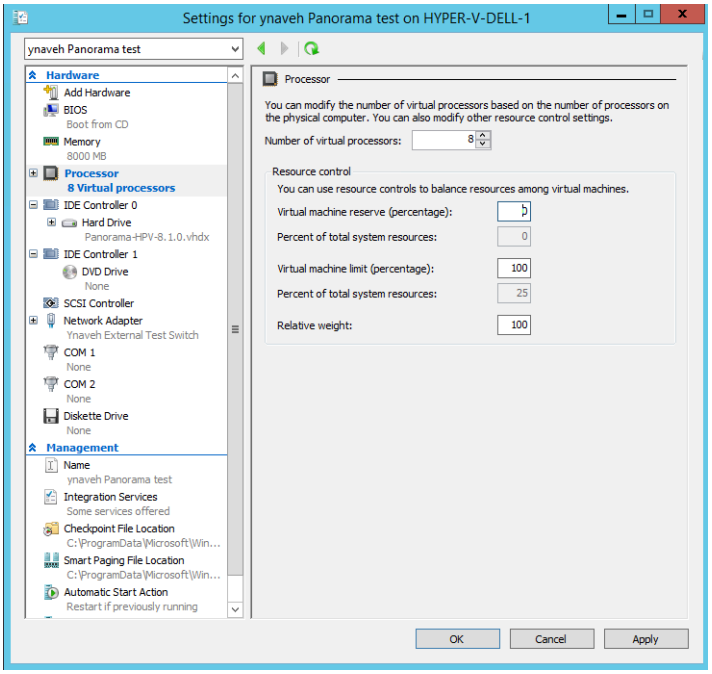
©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama 가상 어플라이언스 CPU 코어를 할당합니다.

최소 리소스 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

Panorama 가상 어플라이언스를 전용 로그 수집기로 사용하려는 경우 초기 배포 중에 필요한 리소스로 어플라이언스를 구성해야 합니다. *Panorama* 가상 어플라이언스는 배포한 후 가상 머신의 크기를 조정하는 경우 로그 수집기 모드로 유지되지 않으며 이로 인해 로그 데이터가 손실됩니다.

1. 하드웨어 목록에서 프로세서를 선택합니다.
2. 현재 할당된 가상 프로세서 수를 편집합니다.



STEP 5 | 방화벽에서 데이터플레인 인터페이스에 대해 하나 이상의 네트워크 어댑터를 연결합니다. 이 작업을 반복하여 Panorama 가상 어플라이언스에 추가 네트워크 인터페이스를 생성합니다.

1. 설정 > 하드웨어 > 하드웨어 추가를 선택한 다음 네트워크 어댑터의 하드웨어 유형을 선택합니다.

   레거시 네트워크 어댑터 및 *SR-IOV*는 지원되지 않습니다. 선택하면 *VM* 시리즈 방화벽이 유지 관리 모드로 부팅됩니다.

2. 확인을 클릭합니다.

STEP 6 | (선택 사항) 로그 수집을 위한 추가 저장소를 추가합니다. 가상 로깅 디스크를 추가하려면 필요에 따라 이 단계를 반복합니다. 관리 전용 모드에서 Panorama 가상 어플라이언스를 배포하려면 6단계를 계속하십시오.

Panorama 모드에서 또는 전용 로그 수집기로 Panorama 가상 어플라이언스를 사용하려는 경우 초기 배포 중에 가상 로깅 디스크를 추가하십시오. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드 리소스 요구 사항을 충족하고 하나 이상의 가상 로깅 디스크를 추가한 경우 초기 배포 시 Panorama 모드에 있습니다. 그렇지 않으면 Panorama 가상 어플라이언스는 기본적으로 관리 전

 ©2024 Palo Alto Networks, Inc.

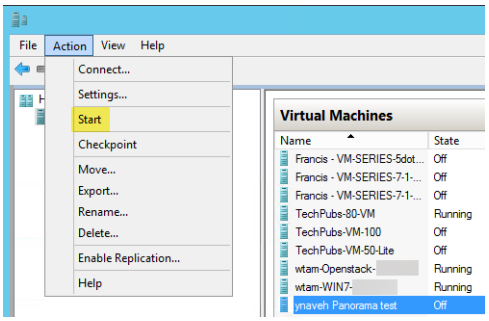
용 모드로 설정됩니다. 디바이스 및 전용 로그 수집기를 관리하고 로컬에서 로그를 수집하지 않으려면 Panorama 가상 어플라이언스를 관리 전용 모드로 변경하십시오.

Hyper-V의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. 2TB보다 작은 로깅 디스크 또는 2TB 로깅 디스크 요구 사항으로 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. Panorama 가상 어플라이언스는 2TB보다 큰 로깅 디스크를 2TB 파티션으로 분할합니다.

1. Hyper-V 관리자에서 호스트를 선택한 다음 작업 > 신규 > 하드 디스크를 선택합니다.
2. 시작하기 전에 프롬프트가 표시되면 다음을 클릭하여 가상 로깅 디스크 추가를 시작합니다.
3. 디스크 형식으로**VHDX**를 선택합니다. 계속하려면 다음을 클릭합니다.
4. 디스크 유형에 대해 필요에 따라 고정 크기 또는 동적 확장을 선택합니다. 계속하려면 다음을 클릭합니다.
5. 가상 로깅 디스크 파일의 이름과 위치를 지정합니다. 계속하려면 다음을 클릭합니다.
6. 디스크를 구성하려면 새 가상 하드 디스크 생성을 선택하고 디스크 크기를 입력합니다. 계속하려면 다음을 클릭합니다.
7. 요약을 검토하고 가상 하드 로깅 디스크 추가를 마칩니다.

STEP 7 | Panorama 가상 어플라이언스의 전원을 켭니다.

1. 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. 작업 > 시작을 선택하여 Panorama 가상 어플라이언스의 전원을 켭니다.



STEP 8 | Hyper-V 관리자에서 파노라마 가상 장치 콘솔에 연결합니다.

1. 가상 머신 목록에서 Panorama 가상 어플라이언스를 선택합니다.
2. 작업 > 연결을 선택한 다음 사용자 이름과 암호를 입력하여 로그인합니다(기본값은 둘 다 admin임).

STEP 9 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 장비의 웹 인터페이스 또는 CLI에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. 새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

Panorama CLI에 처음 로그인할 때 계속하려면 먼저 ###의 이전 암호와 새 암호를 입력하라는 메시지가 표시됩니다.

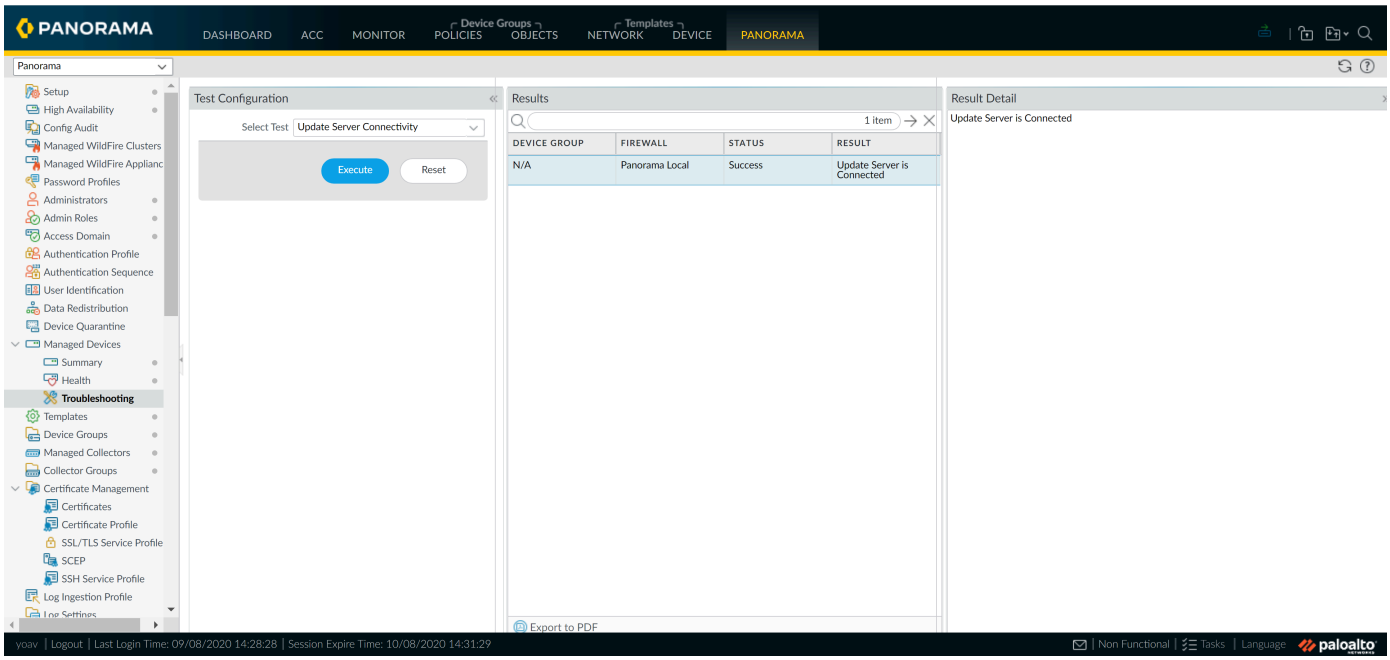
 ©2024 Palo Alto Networks, Inc.

STEP 10 | 관리 인터페이스의 IP 주소를 구성합니다.

1. 다음 명령을 입력합니다. 여기서 *<Panorama-IP>*은(는) 파노라마 관리 인터페이스에 할당하려는 IP 주소이고, *<netmask>*은(는) 서브넷 마스크이며, *<gateway-IP>*은(는) 네트워크 게이트웨이의 IP 주소이고 *<DNS-IP>*은(는) DNS 서버의 IP 주소입니다.

```
admin> configure admin# set deviceconfig system ip-
address <Panorama-IP> netmask <netmask> default-
gateway <gateway-IP> dns-setting servers primary <DNS-IP>
 admin# commit admin# exit
```

2. 네트워크 리소스에 대한 연결 문제 해결 다음 예와 같이 기본 게이트웨이, DNS 서버 및 Palo Alto Networks 업데이트 서버와 같은 방화벽 관리에 필요한 외부 서비스에 대한 네트워크 액세스를 확인합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 11 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

STEP 12 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.

  1. 필요에 따라 Hyper-V의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 ***IP*** 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.

- Panorama 모드의 Panorama용.

  1. Hyper-V의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.

- 관리 전용 모드의 Panorama의 경우.

  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

©2024 Palo Alto Networks, Inc.

Oracle Cloud Infrastructure(OCI)에서 Panorama 설정

OCI(Oracle Cloud Infrastructure)에 Panorama™ 가상 어플라이언스를 설정하여 물리적 방화벽과 VM 시리즈 방화벽의 구성을 중앙에서 관리합니다.

- OCI에 Panorama 가상 어플라이언스 이미지 업로드
- Oracle Cloud Infrastructure(OCI)에 Panorama 설치
- OCI에서 Panorama용 SSH 키 생성

OCI에 Panorama 가상 어플라이언스 이미지 업로드

KVM용 Panorama qcow2 파일을 업로드하고 Panorama 가상 어플라이언스를 시작하는 데 필요한 사용자 지정 이미지를 생성하려면 다음 절차를 완료하십시오. 이미지 업로드 및 생성은 한 번만 필요합니다. Panorama 가상 어플라이언스의 모든 후속 배포에 동일한 이미지를 사용할 수 있습니다.

STEP 1 | Palo Alto Networks CSP(고객 지원 포털)에서 KVM용 Panorama qcow2 파일을 다운로드합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. 업데이트 > 소프트웨어 업데이트를 선택한 다음 소프트웨어 업데이트 필터 드롭다운에서 **Panorama** 기본 이미지를 선택합니다.
3. `Panorama-KVM` qcow2 이미지의 최신 버전을 다운로드합니다.

STEP 2 | Oracle Cloud Infrastructure 콘솔에 로그인합니다.

STEP 3 | qcow2 파일에 대한 스토리지 버킷을 생성합니다.

1. 개체 스토리지 > 개체 스토리지를 선택한 다음 버킷을 생성합니다.
2. 설명이 포함된 버킷 이름을 입력합니다.
3. 스토리지 계층에 대해 표준을 선택합니다.
4. 버킷을 생성합니다.

STEP 4 | qcow2 이미지를 OCI 스토리지 버킷에 업로드합니다.

1. 버킷 세부 정보를 보려면 이전 단계에서 생성한 스토리지 버킷을 클릭합니다.
2. 업로드를 클릭하고 Palo Alto Networks CSP에서 다운로드한 qcow2 이미지를 선택합니다.
3. 이미지를 업로드합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | qcow2 파일에 대한 사전 인증된 요청을 생성합니다.

이는 Panorama 가상 어플라이언스에 대한 사용자 지정 이미지 생성에 사용되는 개체 URL을 생성하는 데 필요합니다.

1. 개체 스토리지 > 개체 스토리지를 선택한 다음 이전 단계에서 생성한 스토리지 버킷을 클릭합니다.
2. 사전 인증된 요청 > 사전 인증된 요청 생성을 선택합니다.
3. 사전 인증된 요청에 대한 설명이 포함된 이름을 입력합니다.
4. 개체를 선택한 다음 개체 이름에 qcow2 이미지 이름을 입력합니다.
5. 사전 인증된 요청을 생성합니다.
6. 액세스 유형에 대해 개체 읽기 및 쓰기 허용을 선택합니다.
7. 만료 날짜와 시간을 입력합니다.
8. 사전 인증된 요청을 생성합니다.
9. 사전 인증된 요청 세부 정보에서 사전 인증된 요청 URL을 복사합니다.

   사전 인증된 요청 *URL*은 사용자 지정 이미지를 생성하는 데 필요하며 표시될 때 복사해야 합니다.

   사전 인증된 요청 *URL*은 요청이 생성된 후에만 표시되며 다시 표시되지 않습니다.
10. URL을 복사한 후 사전 인증된 요청 세부 정보를 닫습니다.

STEP 6 | qcow2 파일을 가져오고 사용자 지정 Panorama 가상 어플라이언스 이미지를 생성합니다.

1. 컴퓨팅 > 사용자 지정 이미지 및 이미지 가져오기를 선택합니다.
2. 이미지에 대한 설명이 포함된 이름을 입력합니다.
3. 개체 스토리지 **URL**에서 가져오기를 선택한 다음 개체 스토리지 URL을 붙여넣습니다.
4. 이미지 유형에서 **QCOW2** 를 선택합니다.
5. 시작 모드의 경우 반가상화 모드를 선택합니다.
6. 이미지 가져오기.

Oracle Cloud Infrastructure(OCI)에 **Panorama** 설치

Oracle Cloud Infrastructure(OCI)에서 Panorama™ 가상 어플라이언스 인스턴스를 생성합니다. OCI 인스턴스는 기본적으로 단일 NIC를 지원합니다. OCI에 Panorama 가상 어플라이언스를 성공적으로 설치하려면 Palo Alto Networks CSP(고객 지원 포털)에서 다운로드한 Panorama 가상 어플라이언스 qcow2 이미지를 OCI에 수동으로 업로드해야 합니다.

OCI에 배포된 Panorama 가상 어플라이언스는 BYOL(Bring Your Own License)이며 모든 배포 모드(Panorama, Log Collector 및 Management Only)를 지원하고 M-시리즈 하드웨어 어플라이언스와 동일한 프로세스 및 기능을 공유합니다. Panorama 모드에 대한 자세한 내용은 Panorama 모델을(를) 참조하십시오.

Linux 운영 체제를 실행하는 시스템은 OCI에 Panorama를 성공적으로 설치해야 합니다. OCI에 Panorama를 성공적으로 설치하려면 OpenSSH를 사용하여 `.pub` 키를 생성해야 합니다. 또한 초기 네트워크 구성을 위해 Linux 시스템만 Panorama CLI에 로그인할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토하여 요구 사항에 필요한 가상 리소스를 결정합니다. Panorama 가상 어플라이언스에 대한 가상 리소스 요구 사항은 Panorama 가상 어플라이언스에서 관리하는 총 방화벽 수와 관리되는 방화벽에서 Log Collector로 로그를 포워딩하는 데 필요한 LPS(초당 로그)를 기반으로 합니다.

Panorama 가상 어플라이언스의 프로비저닝이 부족하면 관리 성능에 영향을 미칩니다. 여기에는 *Panorama* 가상 어플라이언스의 프로비저닝 부족 정도에 따라 *Panorama* 가상 어플라이언스가 느려지거나 응답하지 않는 것이 포함됩니다.

STEP 1 | Oracle Cloud Infrastructure 콘솔에 로그인합니다.

STEP 2 | 네트워크 요구 사항에 맞게 VCN(가상 클라우드 네트워크)을 설정합니다.

기존 VCN에서 Panorama 가상 어플라이언스를 시작하든 새 VCN을 생성하든 Panorama 가상 어플라이언스는 VCN의 다른 인스턴스에서 트래픽을 수신하고 필요에 따라 VCN과 인터넷 간의 인바운드 및 아웃바운드 통신을 수행할 수 있어야 합니다.

자세한 내용은 OCI VCN 설명서를 참조하십시오.

1. VCN을 구성하거나 기존 VCN을 사용합니다.
2. 네트워크 및 보안 구성 요소가 적절하게 정의되었는지 확인합니다.
   - 인터넷 게이트웨이를 생성하여 Panorama 가상 어플라이언스의 서브넷에 대한 인터넷 액세스를 활성화합니다. 소프트웨어 및 콘텐츠 업데이트를 설치하고, 라이선스를 활성화하고,

 ©2024 Palo Alto Networks, Inc.

Palo Alto Networks 클라우드 서비스를 활용하려면 인터넷 액세스가 필요합니다. 그렇지 않으면 수동으로 업데이트를 설치하고 라이선스를 활성화해야 합니다.

Panorama 가상 어플라이언스 인스턴스가 프라이빗 서브넷의 일부인 경우 서브넷에 대해 아웃바운드 인터넷 액세스만 활성화하도록 NAT 게이트웨이를 구성할 수 있습니다.

- 서브넷을 생성합니다. 서브넷은 OCI 인스턴스를 시작할 수 있는 VCN에 할당된 IP 주소 범위의 세그먼트입니다. 필요한 경우 인터넷에 액세스하도록 구성할 수 있도록 Panorama 가상 어플라이언스가 관리 서브넷에 속하는 것이 좋습니다.
- 프라이빗 서브넷의 라우팅 테이블에 경로를 추가하여 VCN의 서브넷과 해당되는 경우 인터넷에서 트래픽을 라우팅할 수 있도록 합니다.

  다음 간의 통신을 허용하려면 서브넷 간에 경로를 생성해야 합니다.

  - Panorama, 관리 방화벽 및 로그 수집기.
  - (선택 사항) Panorama 및 인터넷.
- VCN이 VCN 트래픽을 관리할 수 있도록 다음 수신 보안 규칙이 허용되는지 확인하십시오. 각 규칙의 수신 트래픽 소스는 배포 토폴로지에 고유합니다.

  자세한 내용은 Panorama에 사용되는 포트를 참조하십시오.

  - SSH(포트 **22**) 트래픽을 허용하여 Panorama CLI에 대한 액세스를 활성화합니다.
  - Panorama 웹 인터페이스에 대한 액세스를 활성화하려면 HTTPS(포트 **443** 및 **28270**) 트래픽을 허용합니다.
  - 포트 **3978**의 트래픽을 허용하여 Panorama 간의 통신을 활성화하고 방화벽을 관리하며 로그 수집기를 관리합니다. 이 포트는 또한 로그 수집기가 Panorama로 로그를 포워딩하는 데 사용됩니다.
  - 포트 **28443**에서 트래픽을 허용하여 관리 방화벽이 Panorama에서 소프트웨어 및 콘텐츠 업데이트를 받을 수 있도록 합니다.

STEP 3 | 컴퓨팅 > 인스턴스 및 인스턴스 생성을 선택합니다.

STEP 4 | Panorama 가상 어플라이언스 이미지를 설명하는 이름을 입력합니다.

STEP 5 | 가용성 도메인을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Palo Alto Networks Panoram 이미지를 선택합니다.

*OCI*에서 자체 *Panorama* 가상 어플라이언스 사용자 지정 이미지를 업로드하고 유지 관리하려면 OCI에 Panorama 가상 어플라이언스 이미지 업로드을(를) 참조하십시오

1. 이미지 및 모양에서 이미지 변경을 선택합니다.
2. 이미지 소스의 경우 파트너 이미지를 선택합니다.

   고유한 Panorama 가상 장비 이미지를 유지 관리하는 경우 대신 사용자 지정 이미지를 선택하고 OCI에 업로드한 Panorama 가상 장비 이미지를 선택합니다.
3. **`Palo Alto Networks Panorama`**를 검색하고 이미지를 선택(체크 표시) 합니다.

   이전 단계에서 사용자 정의 이미지를 선택한 경우 이 단계를 건너뜁니다.

   PAN-OS 10.2.0은 기본 PAN-OS 버전입니다.
4. 이미지를 선택합니다.

STEP 7 | 인스턴스 리소스를 구성합니다.

Panorama 사용 요구 사항에 따라 필요한 최소 리소스에 대한 자세한 내용은 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.

1. 이미지 및 모양에서 모양 변경을 선택합니다.
2. 필요한 CPU 수, RAM 크기 및 인터페이스 수로 모양을 선택합니다.
3. 모양을 선택합니다.

STEP 8 | 인스턴스 네트워킹 설정을 구성합니다.

1. 네트워크의 경우 기존 가상 클라우드 네트워크를 선택하고 VCN을 선택합니다.
2. 서브넷의 경우 기존 서브넷을 선택하고 서브넷을 선택합니다.

   필요한 경우 인터넷 액세스를 안전하게 허용하려면 Panorama 가상 어플라이언스 인스턴스를 관리 서브넷에 배포하는 것이 좋습니다.
3. (선택 사항) VCN 외부에서 Panorama 가상 어플라이언스에 액세스할 수 있도록 하려면 공용 IP 주소에서 공용 **IPv4** 주소 할당을 선택합니다.

STEP 9 | Panorama 가상 어플라이언스 인스턴스 부팅 볼륨을 구성합니다.

1. 부팅 볼륨의 경우 사용자 지정 부팅 볼륨 크기를 지정합니다.
2. 부팅 볼륨 크기에 **81**을 입력합니다.

STEP 10 | Panorama 가상 어플라이언스 이미지를 생성합니다.

©2024 Palo Alto Networks, Inc.

STEP 11 | OCI 콘솔에서 Panorama 가상 어플라이언스 CLI에 로그인합니다.

1. OCI에서 Panorama용 SSH 키 생성.
2. OCI 콘솔에서 인스턴스를 선택한 다음 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
3. 콘솔 연결을 선택한 다음 콘솔 연결 생성을 선택합니다.
4. 공개 키 파일**(.pub)** 업로드를 선택한 다음 생성한 공개 SSH 키를 콘솔 연결 생성에 업로드합니다.
5. 인스턴스 세부 정보 화면에서 콘솔 연결 옵션과 **Linux/Mac**용 직렬 연결 복사를 확장합니다.
6. Linux 컴퓨터에서 터미널을 열고 직렬 연결을 붙여넣습니다.

STEP 12 | Panorama 가상 어플라이언스에 대한 새 관리 암호를 구성합니다.

Panorama 가상 장비의 웹 인터페이스 또는 CLI에 액세스하려면 먼저 고유한 관리 암호를 구성해야 합니다. 새 암호는 최소 8자 이상이어야 하며 최소 하나의 소문자, 하나의 대문자, 하나의 숫자 또는 특수 문자를 포함해야 합니다.

Panorama CLI에 처음 로그인할 때 계속하려면 먼저 ###의 이전 암호와 새 암호를 입력하라는 메시지가 표시됩니다.

STEP 13 | Panorama 가상 어플라이언스에 대한 시스템 IP 주소 설정을 구성합니다.

1. Panorama 가상 어플라이언스의 초기 네트워크 설정을 구성합니다.

```
admin> configure
```

```
admin#  set deviceconfig system type static
```

```
admin#  set deviceconfig system ip-address <instance-private-
IP address> netmask <netmask> default-gateway <default-
gateway-IP>
```

```
admin#  set deviceconfig system dns-setting servers primary
 <primary-dns-IP>
```

```
admin#  set deviceconfig system dns-setting servers secondary
 <secondary-dns-IP>
```

```
admin# ##
```

2. Panorama 웹 인터페이스에 로그인할 수 있는지 확인합니다.

   Panorama 웹 인터페이스에 로그인할 수 없는 경우 라우팅 테이블과 VCN 보안 규칙을 검토하여 올바른 경로와 보안 규칙이 생성되었는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 14 | Panorama 가상 어플라이언스를 등록하고 디바이스 관리 라이선스 및 지원 라이선스를 활성화합니다.

1. (VM Flex 라이선스만 해당) Panorama 가상 어플라이언스 일련번호 프로비저닝.

   VM Flex 라이선스를 활용할 때 이 단계는 Panorama 가상 어플라이언스를 Palo Alto Networks CSP(고객 지원 포털)에 등록하는 데 필요한 Panorama 가상 어플라이언스 일련번호를 생성하는 데 필요합니다.

2. Panorama 등록.

   주문 이행 이메일에서 Palo Alto Networks에서 제공한 일련번호를 사용하여 Panorama 가상 어플라이언스를 등록해야 합니다.

   일련번호가 생성될 때 CSP에 자동으로 등록되므로 VM Flex 라이선스를 활용할 때는 이 단계가 필요하지 않습니다.

3. 방화벽 관리 라이선스를 활성화합니다.

   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
   - Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

4. Panorama 지원 라이선스를 활성화합니다.

STEP 15 | 배포 요구 사항에 맞게 Panorama 가상 어플라이언스 구성을 완료합니다.

- 로그 수집기 모드의 Panorama용.
  1. 필요에 따라 Oracle Cloud Infrastructure(OCI)의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Log Collector 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. 6단계에서 시작하여 로그 수집기 모드로 전환합니다.

     Panorama 관리 서버에 로그 수집기를 관리 수집기로 추가할 때 전용 로그 수집기의 공용 ***IP*** 주소를 입력합니다. ***IP*** 주소, 넷마스크 또는 게이트웨이를 지정할 수 없습니다.

- Panorama 모드의 Panorama용.
  1. Oracle Cloud Infrastructure(OCI)의 Panorama에 가상 디스크 추가.

     Panorama 가상 어플라이언스를 Panorama 모드로 변경하려면 하나 이상의 가상 로깅 디스크를 추가해야 합니다.

  2. Panorama 모드에서 Panorama 가상 어플라이언스 설정.
  3. 관리형 수집기 구성.
- 관리 전용 모드의 Panorama의 경우.
  1. 관리 전용 모드에서 Panorama 가상 어플라이언스를 설정합니다.
  2. Panorama 가상 어플라이언스에 전용 로그 수집기를 추가하려면 관리형 수집기 구성.

     관리 전용 모드는 로컬 로그 수집을 지원하지 않으며 관리되는 디바이스 로그를 저장하려면 전용 로그 수집기가 필요합니다.

 ©2024 Palo Alto Networks, Inc.

OCI에서 Panorama용 SSH 키 생성

Oracle Cloud Infrastructure(OCI)에 설치된 Panorama™ 가상 어플라이언스에 연결하려면 Linux 시스템에서 공개 및 개인 SSH 키를 생성해야 합니다. 생성된 SSH 키를 사용하여 Panorama CLI에 로그인하여 새 관리 암호를 설정하고 Panorama 네트워크 설정을 구성합니다.

SSH 키를 생성하고 초기 구성을 위해 *Panorama CLI*에 액세스하려면 *Linux* 시스템이 필요합니다. *OCI* 또는 *PuTTygen*과 같은 타사 애플리케이션에서 *SSH*를 생성하는 것은 지원되지 않습니다.

STEP 1 | Linux 컴퓨터에서 터미널을 엽니다.

STEP 2 | 숨겨진 `.ssh` 디렉토리로 이동합니다.

```
admin:~$ cd ~/.ssh
```

STEP 3 | `.ssh` 디렉토리에 SSH 키를 생성합니다.

```
admin:~/.ssh$ ssh-keygen
```

메시지가 표시되면 기본 `.ssh` 디렉토리에 키를 저장합니다. 키의 암호는 선택 사항입니다.

개인 키의 기본 이름은 `id_rsa`이고 공개 키의 기본 이름은 `id_rsa.pub`입니다.

STEP 4 | `.ssh` 디렉터리의 퍼블릭 키를 홈 디렉터리로 복사합니다.

공개 키를 OCI에 업로드하기 위해 필요한 단계입니다.

```
admin: ~/.ssh$ cp id_rsa.pub ~
```

Panorama 가상 어플라이언스의 초기 구성 수행

Panorama 모델에 따라 Alibaba Cloud Console, AWS, Azure, GCP 또는 OCI 웹 인터페이스, KVM Virtual Machine Manager, Hyper-V Manager, VMware vSphere Client 또는 vCloud Air 웹 콘솔을 사용하여 Panorama 가상 어플라이언스에 대한 네트워크 액세스를 설정합니다. 기본적으로 Panorama 가상 어플라이언스는 Panorama 모드로 배포됩니다. 통합 보고의 경우 Panorama와 모든 관리되는 방화벽 및 로그 수집기에서 GMT(그리니치 표준시) 또는 UTC(협정 세계시)를 균일한 시간대로 사용하는 것이 좋습니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 네트워크 관리자로부터 필요한 정보를 수집하십시오.

관리(MGT) 인터페이스에 대해 다음 정보를 수집합니다.

- 관리(MGT) 인터페이스의 IP 주소

  기본 관리 인터페이스 *IP* 주소는 *192.168.1.1*입니다. Panorama 가상 어플라이언스를 설치할 때 설명한 대로 관리 인터페이스를 구성하지 않은 경우.

- 넷마스크
- 기본 게이트웨이
- DNS 서버 IP 주소

  MGT 인터페이스 구성을 완료하려면 *IP* 주소, 넷마스크*(IPv4*의 경우*)* 또는 접두사 길이*(IPv6*의 경우*)* 및 기본 게이트웨이를 지정해야 합니다. 설정*(*예*:* 기본 게이트웨이*)*을 생략하면 향후 구성 변경을 위해 콘솔 포트를 통해서만 *Panorama*에 액세스할 수 있습니다. 가장 좋은 방법은 항상 완전한 *MGT* 인터페이스 구성을 커밋하는 것입니다.

STEP 2 | Panorama 가상 어플라이언스의 콘솔에 액세스합니다.

Panorama는 관리 트래픽, 고가용성 동기화, 로그 수집 및 수집기 그룹 내 통신을 위해 MGT 인터페이스를 사용합니다.

*PAN-OS 9.0.4*부터는 기본 *###* 자격 증명이 더 이상 지원되지 않습니다. Panorama 가상 어플라이언스를 처음 설치할 때 *Panorama CLI*에 로그인하여 고유한 *###* 암호를 구성해야 합니다.

*Panorama CLI*에 처음 로그인하는 경우 *Panorama* 가상 디바이스의 초기 구성을 계속하기 전에 *###* 사용자의 이전 암호 및 새 암호를 입력하라는 메시지가 표시됩니다.

1. 콘솔에 액세스합니다.

   ESXi 서버에서:

   1. VMware vSphere 클라이언트를 시작합니다.
   2. Panorama 가상 어플라이언스의 콘솔 탭을 선택한 다음 Enter 키를 눌러 로그인 화면에 액세스합니다.

   vCloud Air:

   1. vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud OnDemand** 지역을 선택합니다.
   2. 가상 머신 탭을 선택한 다음 Panorama 가상 머신을 마우스 오른쪽 버튼으로 클릭한 다음 콘솔에서 열기를 선택합니다.

2. 사용자 이름과 비밀번호를 입력하여 로그인합니다(기본값은 둘 다 admin입니다).

   Alibaba Cloud, AWS, Azure, GCP, KVM, Hyper-V 및 OCI:

   - Panorama CLI에 로그인합니다.

 ©2024 Palo Alto Networks, Inc.

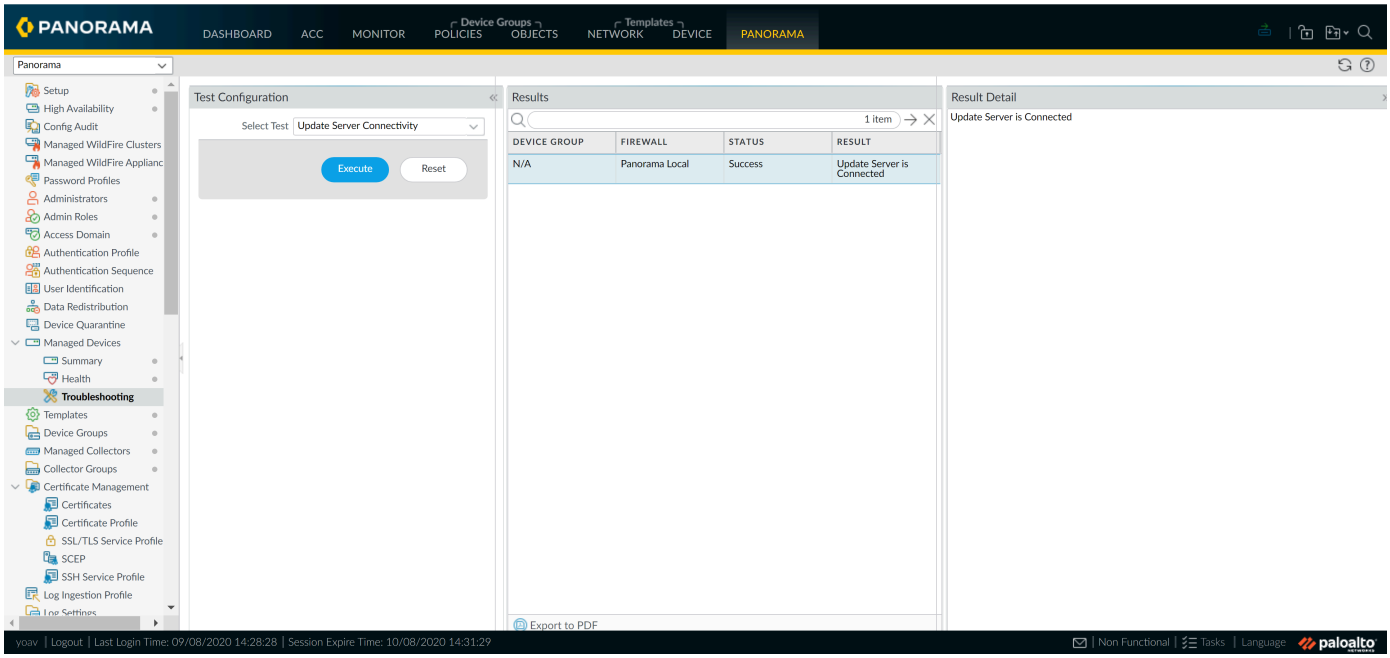
STEP 3 | MGT 인터페이스에 대한 네트워크 액세스 설정을 구성합니다.

Panorama는 관리 트래픽, 고가용성 동기화, 로그 수집 및 수집기 그룹 내 통신을 위해 MGT 인터페이스를 사용합니다.

1. 다음 명령을 입력합니다. 여기서 *<Panorama-IP>*은(는) 파노라마 관리 인터페이스에 할당하려는 IP 주소이고, *<netmask>*은(는) 서브넷 마스크이며, *<gateway-IP>*은(는) 네트워크 게이트웨이의 IP 주소이고 *<DNS-IP>*은(는) DNS 서버의 IP 주소입니다.

```
> configure # set deviceconfig system ip-address <Panorama-IP>
  netmask <netmask> default-gateway <gateway-IP> dns-setting
  servers primary <DNS-IP> # commit # exit
```

2. 네트워크 리소스에 대한 연결 문제 해결 다음 예와 같이 기본 게이트웨이, DNS 서버 및 Palo Alto Networks 업데이트 서버와 같은 방화벽 관리에 필요한 외부 서비스에 대한 네트워크 액세스를 확인합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 일반 설정을 구성합니다.

1. 웹 브라우저에서 보안 연결(HTTPS)을 사용하여 관리 인터페이스에 할당한 IP 주소와 비밀번호(https://<IP address>)를 사용하여 Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
3. 서버의 호스트 이름을 입력하고 네트워크 도메인 이름을 입력합니다. 도메인 이름은 레이블일 뿐입니다. Panorama는 도메인에 가입하는 데 사용하지 않습니다.
4. Panorama의 시계와 관리형 방화벽을 맞춰 동일한 시간대(예: GMT 또는 UTC)를 사용합니다. Strata Logging Service를 사용하려는 경우, Panorama가 Strata Logging Service와 동기화될 수 있도록 NTP를 구성해야 합니다.

   Panorama가 로그를 수신하고 관리되는 방화벽이 로그를 생성할 때 타임스탬프가 기록됩니다. Panorama와 방화벽의 시간대를 맞추면 타임스탬프가 동기화되고 Panorama에서 로그를 쿼리하고 보고서를 생성하는 프로세스가 조화롭게 이루어집니다.
5. 세계 지도에서 Panorama 관리 서버를 정확하게 배치하려면 위도 및 경도를 입력합니다.
6. 주문 처리 이메일에서 받은 일련번호를 입력합니다.
7. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 5 | (선택 사항) 관리 인터페이스 설정을 수정합니다.

IPv6 IP 주소를 사용하여 *Panorama*에 대한 연결을 구성하려면 *IPv6 IP* 주소를 사용하여 *Panorama*를 성공적으로 구성하도록 *IPv4* 및 *IPv6*을 모두 구성해야 합니다. *Panorama*는 *IPv6 IP* 주소만으로 관리 인터페이스를 구성하는 것을 지원하지 않습니다.

1. **Panorama** > 설정 > 인터페이스를 선택한 다음 관리를 클릭합니다.
2. 방화벽이 개인 IP 주소(NAT)로 변환된 공용 IP 주소를 사용하여 Panorama 관리 서버에 연결하는 경우 공용 **IP** 주소 필드에 공용 IP를 입력하고 **IP** 주소 필드에 개인 IP를 입력하여 두 주소를 모두 방화벽에 푸시합니다.
3. 인터페이스(예: **SSH** 액세스)에서 허용할 네트워크 연결 서비스를 선택합니다.

   Telnet 또는 ***HTTP***를 선택하지 마십시오. 이러한 서비스는 일반 텍스트를 사용하며 다른 서비스보다 덜 안전합니다.
4. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.

STEP 6 | 구성 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 다음 단계...

1. 필요한 경우 Panorama 가상 어플라이언스에서 로그 스토리지 용량을 확장합니다.
2. (모범 사례) Panorama가 관리(MGT) 인터페이스를 통해 HTTPS 트래픽을 보호하는 데 사용하는 기본 인증서를 교체합니다.
3. Panorama 지원 라이선스 활성화.
4. Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
5. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.
6. Panorama에 대한 관리 액세스 설정

Panorama 가상 어플라이언스를 로그 수집기로 설정

로그 수집을 위한 전용 가상 어플라이언스를 원하는 경우 로그 수집기 모드에서 ESXi, Alibaba Cloud, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM, Hyper-V 또는 Oracle Cloud Infrastructure(OCI)에서 Panorama 가상 어플라이언스를 구성하십시오. 이렇게 하려면 먼저 라이선스, 소프트웨어 및 콘텐츠 업데이트 설치, 관리(MGT) 인터페이스 구성을 포함하는 Panorama 모드에서 가상 어플라이언스의 초기 구성을 수행합니다. 그런 다음 Panorama 가상 어플라이언스를 Log Collector 모드로 전환하고 Log Collector 구성을 완료합니다. 또한 로그 수집 및 수집기 그룹 통신을 위해 MGT 인터페이스 대신 전용 M-시리즈 어플라이언스 인터페이스(권장)를 사용하려면 먼저 Panorama 관리 서버에 대한 인터페이스를 구성한 다음 로그 수집기에 대해 구성해야 합니다. 그런 다음 Panorama 커밋을 수행한 다음 Collector Group 커밋을 수행합니다.

새 가상 어플라이언스를 Log Collector로 설정하거나 이전에 Panorama 관리 서버로 배포된 기존 가상 어플라이언스를 변환하려면 다음 단계를 수행하십시오.

가상 어플라이언스를 *Panorama* 모드에서 *Log Collector* 모드로 전환하면 어플라이언스가 재부팅되고 로컬 *Log Collector*가 삭제되고 기존 로그 데이터가 삭제되고 관리 액세스 설정을 제외한 모든 구성이 삭제됩니다. 모드를 전환해도 라이선스, 소프트웨어 업데이트 또는 콘텐츠 업데이트는 삭제되지 않습니다.

STEP 1 | 아직 설정하지 않은 경우 Log Collector를 관리할 Panorama 가상 어플라이언스 관리 서버를 설정합니다.

다음 작업 중 하나를 수행합니다.

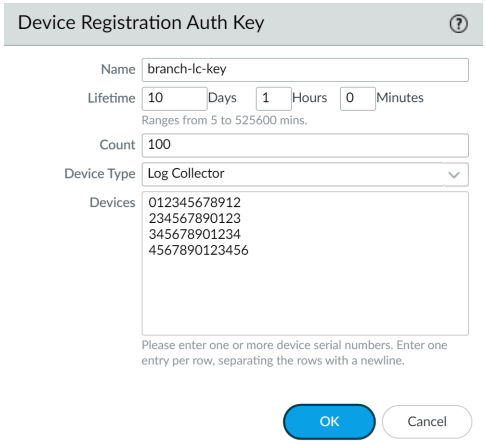
- Panorama 가상 어플라이언스 설정
- M-시리즈 어플라이언스 설정

©2024 Palo Alto Networks, Inc.

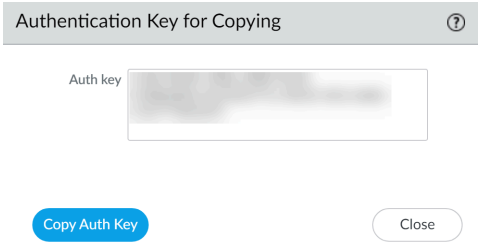
STEP 2 | Panorama 관리 서버에서 디바이스 등록 인증 키를 만들어 전용 로그 수집기를 Panorama 관리에 안전하게 추가합니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
3. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 기간에 대한 키 수명을 지정합니다.
   - 개수 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 로그 수집기를 인증하는 데만 사용되도록 지정합니다.

     모두를 선택하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩하는 디바이스 등록 인증 키를 사용할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 로그 수집기를 지정할 하나 이상의 디바이스 일련번호를 입력합니다.
4. 확인을 클릭합니다.



5. 인증 키를 복사하고 닫습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama 관리 서버의 관리 IP 주소를 기록합니다.

고가용성(HA) 구성에서 Panorama를 배포한 경우 각 HA 피어의 IP 주소가 필요합니다.

1. Panorama 관리 서버의 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 확인하여 단독(비 HA) 또는 활성(HA) Panorama의 **IP** 주소를 기록합니다.
3. HA 배포의 경우 **Panorama** > 고가용성을 선택한 다음 설정 섹션을 선택하여 수동 Panorama의 피어 **HA IP** 주소를 기록합니다.

STEP 4 | 전용 로그 수집기 역할을 할 Panorama 가상 어플라이언스를 설정합니다.

이전에 이 어플라이언스를 Panorama 관리 서버로 배포한 경우 MGT 인터페이스가 이미 구성되어 있고 라이선스와 업데이트가 이미 설치되어 있으므로 이 단계를 건너뛸 수 있습니다.

Log Collector 모드의 Panorama 가상 어플라이언스에는 구성 작업을 위한 웹 인터페이스가 없고 CLI만 있습니다. 따라서 Panorama 가상 어플라이언스에서 모드를 변경하기 전에 Panorama 모드의 웹 인터페이스를 사용하여 다음을 수행하십시오.

1. 다음 지원되는 하이퍼바이저 중 하나에서 Panorama 가상 어플라이언스를 설정합니다.
   - ESXi 서버에 Panorama 설치
   - Alibaba Cloud에 Panorama 설치
   - AWS에 Panorama 설치
   - AWS GovCloud에 Panorama 설치
   - Azure에 Panorama 설치
   - Google Cloud Platform에 Panorama 설치
   - Hyper-V에 Panorama 설치
   - Oracle Cloud Infrastructure(OCI)에서 Panorama 설정
2. Panorama 가상 어플라이언스의 초기 구성 수행.
3. Panorama를 등록하고 라이선스를 설치합니다.
4. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.

STEP 5 | (Azure의 Panorama만 해당) 관리자 암호를 수정합니다.

전용 로그 수집기는 Log Collector 모드로 변경하기 위해 admin Administrator 사용자만 지원합니다. admin 관리자 사용자를 사용하여 로그인할 수 있도록 admin 암호를 수정합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리자를 선택한 다음 관리자를 선택합니다.
3. 암호, 암호 확인을 입력하고 확인을 클릭합니다.
4. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | (Panorama on AWS 및 Azure만 해당) admin 사용자를 제외한 모든 사용자를 삭제합니다.

1. Panorama Web Interface에 관리자로 로그인합니다.
2. **Panorama** > 관리자를 선택합니다.
3. admin을 제외한 기존 관리자를 선택한 다음 삭제합니다.
4. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 7 | Panorama CLI에 로그인합니다.

STEP 8 | Panorama 모드에서 로그 수집기 모드로 전환합니다.

1. 다음 명령을 입력하여 로그 수집기 모드로 전환합니다.

   ```
   > request system system-mode logger
   ```

2. **Y**를 입력하여 모드 변경을 확인합니다. 가상 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 가상 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 확인합니다.

   CMS ### 프롬프트가 표시되면 로그 수집기가 재부팅을 완료하지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 *Enter* 키를 누릅니다.

3. CLI에 다시 로그인합니다.
4. 로그 수집기 모드로의 전환이 성공했는지 확인합니다.

   ```
   > show system info | match system-mode
   ```

   모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

   ```
   system-mode: logger
   ```

STEP 9 | Log Collector와 Panorama 관리 서버 간의 연결을 활성화합니다.

로그 수집기 CLI에서 다음 명령을 입력합니다. 여기서 *<IPaddress1>*은(는) 단독(비HA) 또는 활성(HA) Panorama의 MGT 인터페이스용이고 *<IPaddress2>*은(는) 패시브(HA) Panorama의 MGT 인터페이스용입니다.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 10 | 전용 로그 수집기에 디바이스 등록 인증 키를 추가합니다.

```
admin> request authkey set <auth-key>
```



 ©2024 Palo Alto Networks, Inc.

STEP 11 | 로그 수집기의 일련번호를 기록합니다.

Panorama 관리 서버에서 Log Collector를 관리형 수집기로 추가하려면 일련번호가 필요합니다.

1. Log Collector CLI에서 다음 명령을 입력하여 일련번호를 표시합니다.

```
> show system info | match serial
```

2. 일련번호를 기록하십시오.

STEP 12 | Log Collector를 Panorama 관리 서버에 관리형 수집기로 추가합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 관리형 수집기 추가를 선택합니다.
2. 일반 설정에서 로그 수집기에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
3. **Panorama Server IP** 필드에 단독(비 HA) 또는 활성(HA) Panorama의 IP 주소 또는 FQDN을 입력합니다. HA 배포의 경우 **Panorama Server IP 2** 필드에 패시브 Panorama 피어의 IP 주소 또는 FQDN을 입력합니다.

   이러한 IP 주소는 디바이스 관리 및 디바이스 로그 수집 서비스가 활성화된 Panorama 인터페이스를 지정해야 합니다. 기본적으로 이러한 서비스는 MGT 인터페이스에서만 활성화됩니다. 그러나 Panorama 관리 서버인 M-Series Appliance를 설정할 때 다른 인터페이스에서 서비스를 활성화했을 수 있습니다.
4. 인터페이스를 선택한 다음 관리를 클릭한 후 전용 로그 수집기의 공용 **IP** 주소를 입력합니다.
5. 확인을 두 번 클릭하여 변경 사항을 로그 수집기에 저장합니다.
6. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.
7. **Panorama** > 관리형 수집기에 추가한 로그 수집기가 나열되는지 확인합니다. 연결됨 열에는 로그 수집기가 Panorama에 연결되었음을 나타내는 확인 표시가 표시됩니다. 페이지에 업데이트된 연결 상태가 표시될 때까지 몇 분 정도 기다려야 할 수 있습니다.

   이 시점에서 구성 상태 열에는 동기화되지 않음이 표시되고 런타임 상태 열에는 연결 끊김이 표시됩니다. 수집기 그룹을 구성하면 상태가 동기화 중 및 연결됨으로 변경됩니다.

STEP 13 | 로깅 디스크를 활성화합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
2. 디스크를 선택한 다음 각 디스크를 추가합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

©2024 Palo Alto Networks, Inc.

STEP 14 | (권장) Panorama 관리 서버 및 로그 수집기가 디바이스 로그 수집(방화벽에서 로그 수신) 및 수집기 그룹 통신에 사용할 경우**Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** 및 **Ethernet5** 인터페이스를 구성합니다.

이전에 Log Collector를 Panorama 관리 서버로 배포하고 이러한 인터페이스를 구성한 경우 Log Collector 모드로 전환하면 관리 액세스 설정을 제외한 모든 구성이 삭제되므로 다시 구성해야 합니다.

1. 아직 구성하지 않은 경우 Panorama 관리 서버에서 각 인터페이스(MGT 인터페이스 제외)를 구성합니다.
   1. **Panorama** > **Setup** > **Interfaces**를 선택한 다음 인터페이스 이름을 클릭합니다.
   2. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
   3. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.
      - ESXi의 경우
        - IPv4—공용 **IP** 주소, **IP** 주소, 넷마스크 및 기본 게이트웨이

          IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
      - Alibaba Cloud, AWS, Azure, GCP 및 OCI용
        - 공개 **IP** 주소
   4. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 관리 및 디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.

      디바이스 배포(소프트웨어 및 콘텐츠 업데이트) - 하나의 인터페이스만 할당할 수 있습니다.
   5. 확인을 클릭하여 변경 사항을 저장합니다.
2. Log Collector의 각 인터페이스(MGT 인터페이스 제외)를 구성합니다.
   1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
   2. 인터페이스를 선택한 다음 인터페이스 이름을 클릭합니다.
   3. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
   4. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.
      - ESXi의 경우
        - IPv4—공용 **IP** 주소, **IP** 주소, 넷마스크 및 기본 게이트웨이

          IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
      - Alibaba Cloud, AWS, Azure, GCP 및 OCI용
        - 공개 **IP** 주소
   5. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.
   6. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
3. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.

 ©2024 Palo Alto Networks, Inc.

4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 15 | (선택 사항) 배포에서 Panorama와 관리되는 디바이스 간의 인증에 사용자 지정 인증서를 사용하는 경우 사용자 지정 클라이언트 디바이스 인증서를 배포합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택한 다음 드롭다운에서 인증서 프로파일을 선택하거나 새 인증서 프로파일을 클릭하여 생성합니다.
2. 로그 수집기에 대하여 **Panorama** > 관리형 수집기 > 통신 > 추가를 선택합니다.
3. 보안 클라이언트 통신 체크박스를 선택합니다.
4. 유형 드롭다운에서 디바이스 인증서 유형을 선택합니다.
   - 로컬 디바이스 인증서를 사용하는 경우 해당 드롭다운에서 인증서 및 인증서 프로파일을 선택합니다.
   - SCEP를 디바이스 인증서로 사용하는 경우 해당 드롭다운에서 **SCEP** 프로파일 및 인증서 프로파일을 선택합니다.
5. 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 16 | (선택 사항) 로그 수집기에서 보안 서버 통신을 구성합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 관리형 수집기 > 통신 > 추가를 선택합니다.
2. 사용자 지정 인증서만 확인란이 선택되어 있지 않은지 확인합니다. 이를 통해 사용자 지정 인증서로 마이그레이션하는 동안 모든 디바이스를 계속 관리할 수 있습니다.

   Custom Certificate Only 확인란을 선택하면 *Log Collector*가 인증되지 않고 사전 정의된 인증서를 사용하여 디바이스에서 로그를 수신할 수 없습니다.
3. SSL/TLS 서비스 프로파일 드롭다운에서 **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 로그 수집기와 로그를 보내는 디바이스 간의 모든 SSL 연결에 적용됩니다.
4. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
5. 서버가 관리되는 디바이스의 일련번호에 대해 클라이언트를 확인하도록 하려면 일련번호를 기반으로 클라이언트 인증을 선택합니다. 클라이언트 인증서에는 일련번호를 기반으로 권한을 부여하는 CN으로 특수 키워드 $UDID가 설정되어 있어야 합니다.
6. 연결 끊기 대기 시간(분)에 Panorama가 관리형 디바이스와의 연결을 끊고 다시 설정하기 전에 기다려야 하는 시간(분)을 입력합니다. 이 필드는 기본적으로 비어 있으며 범위는 0~44,640분입니다.

   연결 해제 대기 시간은 새 구성을 커밋할 때까지 카운트다운을 시작하지 않습니다.
7. (선택 사항) 권한 부여 목록을 구성합니다.
   1. 인증 목록에서 추가를 클릭합니다.
   2. 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 선택한 유형의 식별자를 입력합니다.
   4. 확인을 클릭합니다.
   5. 권한 부여 목록 확인을 선택하여 권한 부여 목록을 시행하십시오.
8. 확인을 클릭합니다.
9. 커밋 > **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 17 | 수집기 그룹에 로그 수집기를 할당합니다.

1. 수집기 그룹을 구성합니다. Panorama 커밋을 수행한 다음 수집기 그룹 커밋을 수행하여 로그 수집기 구성을 Panorama와 동기화하고 Eth1, Eth2, Eth3, Eth4 및 Eth5 인터페이스(구성한 경우)를 로그 수집기에서 작동 상태로 전환해야 합니다.

   모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.

   단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화하는 것이 가장 좋습니다. 이 옵션을 사용하려면 각 로그 수집기에 동일한 수의 로깅 디스크가 있어야 합니다.

2. **Panorama** > 관리형 수집기를 선택하여 로그 수집기 구성이 Panorama와 동기화되었는지 확인합니다.

   구성 상태 열은 동기화 중으로 표시되어야 하고 런타임 상태 열은 연결됨으로 표시되어야 합니다.

3. Log Collector CLI에 액세스하고 다음 명령을 입력하여 해당 인터페이스가 작동하는지 확인합니다.

   ```
   > show interface all
   ```

   출력은 ## 중인 각 인터페이스에 대해 작동 ##를 표시합니다.

4. 수집기 그룹에 여러 로그 수집기가 있는 경우 네트워크 리소스에 대한 연결 문제 해결 로그 수집기가 사용하는 각 인터페이스에 대해 Ping 연결 테스트를 수행하여 서로 통신할 수 있는지 확인합니다. ## IP 주소에 대해 로그 수집기 중 하나의 인터페이스를 지정합니다. ### IP 주소에 대해 동일한 수집기 그룹에 있는 다른 로그 수집기와 일치하는 인터페이스를 지정합니다.

STEP 18 | 다음 단계...

Log Collector가 방화벽 로그를 수신하도록 하려면:

1. Panorama에 대한 로그 포워딩을 구성합니다.
2. Panorama로 로그 포워딩 확인.

로컬 로그 수집기로 Panorama 가상 어플라이언스 설정

Panorama 8.0 또는 이전 릴리스에서 Panorama 8.1(이상 버전) 릴리스로 업그레이드한 후 Panorama 가상 어플라이언스가 레거시 모드인 경우 로컬 로그 수집기를 생성하고 기존 로그를 잃지 않고 여러 로깅 디스크를 추가하려면 Panorama 모드로 전환하십시오. 로그 스토리지를 최대 24TB까지 늘리고 보고서 생성 속도를 높일 수 있습니다.

레거시 모드에서 *Panorama* 모드로 변경하면 레거시 모드를 더 이상 사용할 수 없습니다.

Panorama 8.1로 업그레이드한 후 첫 번째 단계는 가상 어플라이언스의 시스템 리소스를 Panorama 모드에 필요한 최소 수준으로 늘리는 것입니다. 리소스를 늘리면 Panorama가 재부팅되므로 유지 관리 기간 동안 이 절차를 수행하십시오. 더 큰 시스템 디스크(81GB)를 설치하고, 로그 저장 용량에 따라 CPU와 메모

 ©2024 Palo Alto Networks, Inc.

리를 늘리고, 가상 로깅 디스크를 추가해야 합니다. 새 로깅 디스크의 용량은 어플라이언스가 현재 레거시 모드에서 사용하는 용량 이상이어야 하며 2TB보다 작아서는 안 됩니다. 가상 디스크를 추가하면 기존 로그를 Log Collector로 마이그레이션하고 Log Collector에서 새 로그를 저장할 수 있습니다.

Panorama가 HA 구성으로 배포된 경우 보조 피어에서 먼저 다음 단계를 수행한 다음 기본 피어에서 다음 단계를 수행합니다.

STEP 1 | 가상 어플라이언스가 Panorama 모드에서 작동하기 전에 늘려야 하는 시스템 리소스를 결정합니다.

*Panorama*에 이미 충분한 리소스가 있다고 판단한 경우에도 이 단계에서 지정된 명령을 실행해야 합니다.

1. Panorama CLI에 액세스:
   1. PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 Panorama MGT 인터페이스에 대해 지정한 IP 주소에 대한 SSH 세션을 엽니다.
   2. 메시지가 표시되면 CLI에 로그인합니다.
2. 다음 명령을 실행하여 늘려야 하는 리소스를 확인합니다.

```
> request system system-mode panorama
```

계속할지 묻는 메시지가 표시되면 **y**를 입력합니다. 출력은 늘려야 하는 리소스를 지정합니다. 예:

```
Panorama ### ### 52.0GB# ## ### ###### #### ####. ### 81.0GB# #
### ### ## '### ## ### ### ##'# #### ## ### #### #########. ## ###
 50.00GB# #### # ## ## #### #####. CPU ### #### ##: ## 4# ##, ## 8# #
#
```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | CPU와 메모리를 늘리고 시스템 디스크를 더 큰 디스크로 교체하십시오.

1. VMware ESXi vSphere Client에 액세스하고 가상 머신을 선택한 다음 Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.
2. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
3. 메모리를 선택하고 새 메모리 크기를 입력합니다.
4. **CPU**를 선택한 다음 CPU 수(가상 소켓 수에 소켓당 코어 수를 곱한 값)를 지정합니다.
5. 가상 디스크를 추가합니다.

   이 디스크를 사용하여 기존 시스템 디스크를 교체합니다.

   1. 하드웨어 설정에서 디스크 추가, 하드웨어 유형으로 하드 디스크를 선택한 후 다음을 클릭합니다.
   2. 새 가상 디스크를 생성하고 다음을 클릭합니다.
   3. 디스크 크기를 정확히 81GB로 설정하고 **Thick Provision Lazy Zeroed** 디스크 형식을 선택합니다.
   4. 데이터 저장소 또는 데이터 저장소 구조를 위치로 지정을 선택한 다음 81GB 이상의 데이터 저장소로 이동한 후 확인을 클릭하고 다음을 클릭합니다.
   5. SCSI 가상 디바이스 노드를 선택한 후(기본 선택을 사용할 수 있음) 다음을 클릭합니다.

      SCSI 이외의 형식을 선택하면 *Panorama*가 부팅되지 않습니다.

   6. 설정이 올바른지 확인한 다음 마침 및 확인을 클릭합니다.
6. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다. 계속하기 전에 Panorama가 재부팅될 때까지 기다리십시오.
7. Panorama CLI로 돌아가 원래 시스템 디스크의 데이터를 새 시스템 디스크로 복사합니다.

   ```
   > request system clone-system-disk target sdb
   ```

   계속할지 묻는 메시지가 표시되면 **y**를 입력합니다.

   복사 프로세스는 Panorama가 재부팅되는 동안 약 20~25분이 소요됩니다. 프로세스가 완료되면 출력에 Panorama를 종료하라는 메시지가 표시됩니다.
8. vSphere Client 콘솔로 돌아가서 Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.
9. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
10. 원본 시스템 디스크를 선택한 다음 제거를 클릭하고 가상 머신에서 제거를 선택한 다음 확인을 클릭합니다.
11. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
12. 새 시스템 디스크를 선택한 다음 가상 디바이스 노드를 **SCSI (0:0)**로 설정한 다음 확인을 클릭합니다.
13. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다. 계속하기 전에 Panorama가 새 시스템 디스크에서 재부팅될 때까지 기다립니다(약 15분).

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 가상 로깅 디스크를 추가합니다.

기존 로그를 마이그레이션할 디스크입니다.

1. VMware ESXi vSphere Client에서 Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.
2. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
3. 가상 디스크 추가 단계를 반복합니다. 필요한 로그 스토리지의 양에 따라 디스크 크기를 2TB의 배수로 설정합니다. 용량은 Panorama가 현재 로그에 사용하는 기존 가상 디스크 또는 NFS 스토리지만큼 커야 합니다. 디스크 용량은 2TB의 배수여야 하며 최대 24TB까지 가능합니다. 예를 들어 기존 디스크에 5TB의 로그 스토리지가 있는 경우 최소 6TB의 새 디스크를 추가해야 합니다.

   Panorama 모드로 전환하면 Panorama는 자동으로 새 디스크를 2TB 파티션으로 분할하고 각 파티션은 별도의 가상 디스크로 작동합니다.
4. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다. 계속하기 전에 Panorama가 재부팅될 때까지 기다리십시오.

STEP 4 | 레거시 모드에서 Panorama 모드로 전환합니다.

모드를 전환한 후 어플라이언스는 다시 재부팅되고 로컬 로그 수집기 및 수집기 그룹을 자동으로 생성합니다. 기존 로그는 이 절차의 뒷부분에서 마이그레이션할 때까지 쿼리 또는 보고에 사용할 수 없습니다.

1. Panorama CLI로 돌아가 다음 명령을 실행합니다.

```
> request system system-mode panorama
```

   계속할지 묻는 메시지가 표시되면 **y**를 입력합니다. 재부팅 후 Panorama는 자동으로 로컬 로그 수집기(Panorama라는 이름)를 생성하고 이를 포함할 수집기 그룹(기본 이름)을 생성합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama는 또한 추가한 가상 로깅 디스크를 구성하고 별도의 2TB 디스크로 나눕니다. 계속하기 전에 프로세스가 완료되고 Panorama가 재부팅될 때까지(약 5분) 기다리십시오.

2. Panorama 웹 인터페이스에 로그인합니다.
3. 대시보드의 일반 정보 설정에서 모드가 이제 **Panorama**인지 확인합니다.

   HA 배포에서 보조 피어는 해당 모드(Panorama)가 기본 피어(레거시)의 모드와 일치하지 않기 때문에 이 시점에서 일시 중단된 상태입니다. 이 절차의 뒷부분에서 기본 피어를 Panorama 모드로 전환한 후 보조 피어의 일시 중단을 해제합니다.
4. 기본 수집기 그룹이 생성되었고 로컬 로그 수집기가 기본 수집기 그룹의 일부인지 확인하려면 **Panorama** > 수집기 그룹을 선택합니다.
5. 관리되는 디바이스에 구성을 푸시합니다.
   - 보류 중인 변경 사항이 없는 경우 다음을 따릅니다.
     1. 커밋 > 디바이스에 푸시를 선택한 다음 선택 사항을 편집합니다.
     2. 수집기 그룹을 선택한 다음 기본 수집기 그룹이 선택되어 있는지 확인합니다.
     3. 확인 및 푸시를 클릭합니다.
   - 보류 중인 변경 사항이 있는 경우 다음을 따릅니다.
     1. 커밋 > 커밋 및 푸시 및 편집 선택을 선택합니다.
     2. 디바이스 그룹 디바이스 및 템플릿이 포함되어 있는지 확인합니다.
     3. 수집기 그룹을 선택한 다음 기본 수집기 그룹이 선택되어 있는지 확인합니다.
     4. 확인 및 커밋 및 푸시를 클릭합니다.
6. **Panorama** > 관리형 수집기를 선택한 다음 열에 로컬 로그 수집기에 대한 다음 정보가 표시되는지 확인합니다.
   - 수집기 이름 - 기본적으로 Panorama 호스트 이름입니다. 기본 수집기 그룹 아래에 나열되어야 합니다.
   - 연결됨 - 확인 표시
   - 구성 상태 - 동기화 중
   - 런타임 상태 - 연결됨

©2024 Palo Alto Networks, Inc.

STEP 5 | (HA만 해당) 기본 Panorama를 레거시 모드에서 Panorama 모드로 전환합니다.

이 단계는 페일오버를 트리거합니다.

1. 기본 Panorama에서 1단계~4단계를 반복합니다.

   기본 Panorama가 재부팅되고 활성 HA 상태로 돌아갈 때까지 기다립니다. 선점이 활성화되지 않은 경우 수동으로 장애 복구해야 합니다. **Panorama** > **High Availability**를 선택한 다음 Operational Commands 섹션에서 **Make local Panorama** 기능을 선택합니다.
2. 기본 Panorama에서 대시보드를 선택한 다음 고가용성 섹션에서 피어에 동기화를 클릭하고 예를 클릭하고 실행 중인 구성이 동기화됨 상태를 표시할 때까지 기다립니다.
3. 보조 Panorama에서 **Panorama** > 고가용성을 선택한 다음 작동 명령 섹션에서 로컬 **Panorama**로 설정 기능을 선택합니다.

   이 단계는 보조 Panorama를 일시 중단된 HA 상태에서 해제하는 데 필요합니다.

STEP 6 | 기존 로그를 새 가상 로깅 디스크로 마이그레이션합니다.

HA 구성에서 Panorama를 배포한 경우 기본 피어에서만 이 작업을 수행합니다.

*Palo Alto Networks*는 유지 관리 기간 동안 기존 로그를 새 가상 로깅 디스크로 마이그레이션할 것을 권장합니다. 로그 마이그레이션을 실행하려면 많은 수의 *Panorama* 가상 어플라이언스 *CPU* 코어가 필요하며 *Panorama* 운영 성능에 영향을 미칩니다.

1. Panorama CLI로 돌아갑니다.
2. 로그 마이그레이션 시작:

   ```
   > request logdb migrate vm start
   ```

   프로세스 기간은 마이그레이션하는 로그 데이터의 양에 따라 다릅니다. 마이그레이션 상태를 확인하려면 다음 명령어를 실행하세요.

   ```
   > request logdb migrate vm status
   ```

   마이그레이션이 완료되면 출력에 다음이 표시됩니다. ###### ##되었습니다.
3. 기존 로그를 사용할 수 있는지 확인합니다.
   1. Panorama 웹 인터페이스에 로그인합니다.
   2. **Panorama** > **Monitor**를 선택한 다음 일부 기존 로그(예: **Panorama** > **Monitor** > **System**)와 일치하는 로그 유형을 선택한 다음 로그가 표시되는지 확인합니다.

STEP 7 | 다음 단계...

Log Collector가 방화벽에서 새 로그를 수신하도록 Panorama로의 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 모드에서 Panorama 가상 어플라이언스 설정

Panorama 모드를 사용하면 Panorama™ 가상 어플라이언스가 로컬 로그 수집 기능이 있는 Panorama 관리 서버로 작동할 수 있습니다. 기본적으로 Panorama 가상 어플라이언스는 하나 이상의 가상 로깅 디스크가 Panorama 가상 어플라이언스에 연결된 경우 Panorama 모드로 배포됩니다.

계속 지원되지만 *50GB* 로깅 디스크가 있는 레거시 모드에서 *Panorama* 모드로 전환하는 것은 프로덕션 환경에 권장되지 않습니다. *50GB* 로깅 디스크로 *Panorama* 모드로 전환하면 추가 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Panorama CLI에 로그인합니다.

STEP 2 | Panorama 모드로 전환합니다.

1. Panorama 모드로 변경:

```
> request system system-mode panorama
```

2. **Y**를 입력하여 모드 변경을 확인합니다. Panorama 가상 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 Panorama 가상 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 확인합니다.

   CMS ### 프롬프트가 표시되면 Panorama 가상 어플라이언스의 재부팅이 완료되지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 Enter 키를 누릅니다.

STEP 3 | Panorama 모드로의 전환이 성공했는지 확인합니다.

1. CLI에 다시 로그인합니다.
2. Panorama 모드로의 전환이 성공했는지 확인합니다.

```
> show system info | match system-mode
```

모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

```
> system mode:panorama
```

관리 전용 모드에서 Panorama 가상 어플라이언스 설정

관리 전용 모드를 사용하면 Panorama 가상 어플라이언스가 로컬 로그 수집 기능 없이 Panorama 관리 서버로 엄격하게 작동할 수 있습니다. 기본적으로 Panorama 가상 어플라이언스는 초기 배포의 Panorama 모드에 있습니다. 관리 전용 모드로 변경하려면 관리 전용 모드의 Panorama 가상 어플라이언스가 로그 수집을 지원하지 않기 때문에 Panorama 관리 서버로 포워딩되는 로그가 없어야 하므로 초기 배포 직후 Panorama 가상 어플라이언스를 관리 전용으로 변경하는 것이 좋습니다. 관리 전용 모드로 변경하면 Panorama 가상 어플라이언스에 저장된 기존 로그 데이터에 액세스할 수 없게 되며 ACC 및 보고 기능은 Panorama 가상 어플라이언스에 저장된 로그를 쿼리할 수 없습니다.

(레거시 모드의 Panorama) Panorama 가상 어플라이언스를 레거시 모드에서 관리 전용 모드로 변경할 때 Panorama 가상 어플라이언스에 영향을 주지 않습니다. 예방 조치로 Palo Alto Networks는 예기치 않은

 ©2024 Palo Alto Networks, Inc.

영향이 발생할 경우 Panorama를 복원하는 데 사용할 수 있는 Panorama 가상 어플라이언스의 가상 머신 스냅샷을 찍을 것을 권장합니다.

로컬 로그 수집기를 구성한 경우 로그 수집 기능이 없음에도 불구하고 관리 전용 모드로 변경하면 로컬 로그 수집기가 *Panorama*에 계속 존재합니다. 로컬 로그 수집기(***Panorama*** > 관리형 수집기)를 삭제하면 로컬 로그 수집기가 기본적으로 사용하는 *Eth1/1* 인터페이스 구성이 삭제됩니다. 로컬 로그 수집기를 삭제하려면 Eth1/1 인터페이스를 재구성해야 합니다.

STEP 1 | Panorama CLI에 로그인합니다.

STEP 2 | 관리 전용 모드로 전환합니다.

1. 관리 전용 모드로 변경:

```
> request system system-mode management-only
```

2. **Y**를 입력하여 모드 변경을 확인합니다. Panorama 가상 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 Panorama 가상 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 확인합니다.

   CMS ### 프롬프트가 표시되면 Panorama 가상 어플라이언스의 재부팅이 완료되지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 Enter 키를 누릅니다.

STEP 3 | 관리 전용 모드로의 전환이 성공했는지 확인하십시오.

1. CLI에 다시 로그인합니다.
2. 관리 전용 모드로의 전환이 성공했는지 확인합니다.

```
> show system info | match system-mode
```

   모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

```
> system mode:management-only
```

Panorama 가상 어플라이언스에서 로그 스토리지 용량 확장

Panorama Virtual Appliance의 초기 구성을 수행한 후 사용 가능한 로그 스토리지 용량과 확장 옵션은 가상 플랫폼(VMware ESXi, vCloud Air, Alibaba Cloud, AWS, AWS GovCloud, Azure, Google Cloud Platform, KVM, Hyper-V 또는 OCI) 및 모드(레거시, Panorama 또는 로그 수집기 모드)입니다. 자세한 내용은 Panorama 모델을 참조하십시오.

Panorama 가상 어플라이언스에서 로그 저장 용량을 확장하려면 추가 로깅 디스크를 추가해야 합니다. 기존 로깅 디스크의 로그 저장 용량 확장은 지원되지 않으며, Panorama는 추가 저장 용량을 인식하지 못합니다. 예를 들어; 2TB 로깅 디스크를 추가한 다음 기존 로깅 디스크를 4TB로 확장한 경우 Panorama는 로깅 디스크에 2TB의 저장 용량이 있는 것으로 계속 인식하고 추가 2TB의 저장 용량을 무시합니다.

추가 로그 저장을 위해 방화벽 로그를 전용 로그 수집기로 포워딩하거나(관리 수집기 구성 참조) Panorama에서 외부 대상으로 로그 포워딩을 구성할 수도 있습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama에서 로그 저장 용량을 확장하기 전에 Panorama 로그 저장 요구 사항을 결정하십시오.

- 레거시 모드에서 Panorama 가상 어플라이언스에 스토리지를 추가할 때 기존 로그 보존
- ESXi 서버의 Panorama에 가상 디스크 추가
- vCloud Air의 Panorama에 가상 디스크 추가
- Alibaba Cloud의 Panorama에 가상 디스크 추가
- AWS의 Panorama에 가상 디스크 추가
- Azure의 Panorama에 가상 디스크 추가
- Google Cloud Platform의 Panorama에 가상 디스크 추가
- KVM의 Panorama에 가상 디스크 추가
- Hyper-V의 Panorama에 가상 디스크 추가
- Oracle Cloud Infrastructure(OCI)의 Panorama에 가상 디스크 추가
- NFS 데이터 저장소에 Panorama ESXi 서버 탑재

레거시 모드에서 **Panorama** 가상 어플라이언스에 스토리지를 추가할 때 기존 로그 보존

레거시 모드의 Panorama 가상 어플라이언스는 로깅에 가상 디스크를 하나만 사용할 수 있습니다. 따라서 로깅 전용 가상 디스크를 추가하면 Panorama는 시스템 디스크의 기본 11GB 로그 스토리지 사용을 중지하고 기존 로그를 새 로깅 디스크에 자동으로 복사합니다. (Panorama는 로그 이외의 데이터에 시스템 디스크를 계속 사용합니다.)

최대 2TB 저장 용량의 기존 전용 로깅 디스크를 최대 8TB 디스크로 교체하면 기존 디스크의 로그가 손실됩니다. 로그를 보존하려면 다음을 선택하십시오.

- 가상 디스크를 교체하기 전에 외부 대상에 대한 로그 포워딩을 구성하십시오.

- 새 8TB 디스크에 대한 새 Panorama 가상 어플라이언스를 설정하고 로그가 필요한 동안 이전 디스크가 포함된 Panorama에 대한 액세스를 유지하십시오. 방화벽 로그를 새 Panorama 가상 어플라이언스로 포워딩하려면 새 Panorama IP 주소에 연결하도록 방화벽을 재구성하고(디바이스 > 설정 > 관리 선택 및 Panorama 설정 편집) 방화벽을 새 Panorama에 관리형 디바이스로 추가하고 Panorama에 대한 로그 포워딩 구성을(를) 합니다. 새 Panorama에서 이전 Panorama IP 주소를 재사용하려면 이전 Panorama의 구성을 내보낸 다음 새 Panorama에서 구성을 가져와 로드하는 또 다른 옵션이 있습니다.

- 이전 디스크에서 새 디스크로 로그를 복사합니다. 디스크에 현재 저장되어 있는 로그 수에 따라 복사하는 데 몇 시간이 걸릴 수 있으며 Panorama는 프로세스 중에 로그를 수집할 수 없습니다. 지침은 Palo Alto Networks 고객 지원에 문의하십시오.

ESXi 서버의 **Panorama**에 가상 디스크 추가

Panorama 가상 어플라이언스에서 로그 스토리지 용량을 확장하기 위해 가상 로깅 디스크를 추가할 수 있습니다. 어플라이언스가 Panorama 모드인 경우 각각 2TB의 가상 로깅 디스크 1~12개 또는 최대 총 24TB까지 24TB 로깅 디스크 1개를 추가할 수 있습니다. 어플라이언스가 레거시 모드인 경우 ESXi 5.5 이상의 버전에서 최대 8TB의 가상 로깅 디스크 하나를 추가하거나 이전 ESXi 버전에서 최대 2TB의 디스크 하나를 추가할 수 있습니다. 또한 프로비저닝 형식이 다른 여러 디스크가 있을 때 발생할 수 있는 예기치 않은 성능을 방지하기 위해 동일한 디스크 프로비저닝 형식의 로깅 디스크를 추가하는 것이 권장됩니다.

 ©2024 Palo Alto Networks, Inc.

*Panorama*에서 새 가상 디스크에 대한 연결이 끊어지면 *Panorama*에서 오류 간격 동안 로그가 손실될 수 있습니다.

중복성을 허용하려면 *RAID* 구성에서 가상 디스크를 사용하십시오. *RAID10*은 로깅 특성이 높은 애플리케이션에 대해 최고의 쓰기 성능을 제공합니다.

필요한 경우 ESXi 서버에서 가상 디스크를 교체할 수 있습니다.

STEP 1 | Panorama에 추가 디스크 추가

모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. VMware vSphere Client에 액세스하고 가상 머신을 선택합니다.
2. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고전원 > 전원 끄기를 선택합니다.
3. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다.
4. 하드웨어 탭에서 추가를 클릭하여 하드웨어 추가 마법사를 시작합니다.
5. 하드웨어 유형으로 하드 디스크를 선택하고 다음을 클릭합니다.
6. 새 가상 디스크를 생성하고 다음을 클릭합니다.
7. 디스크 크기를 설정합니다. Panorama 가상 어플라이언스가 Panorama 모드인 경우 크기를 2TB 이상으로 설정합니다. 디바이스가 레거시 모드인 경우 최대 8TB까지 크기를 설정할 수 있습니다.

   Panorama 모드에서는 *2TB*보다 큰 디스크 크기를 추가할 수 있으며 *Panorama*는 가능한 한 많은 *2TB* 파티션을 자동으로 생성합니다. 예를 들어 디스크 *sdc*가 *24TB*인 경우 *12*개의 *2TB* 파티션이 생성됩니다. 이러한 디스크의 이름은 *sdc1-12*입니다.
8. 디스크 프로비저닝 형식을 선택하고 다음을 클릭합니다.
9. 데이터 저장소 또는 데이터 저장소 구조를 지정하고 지정된 디스크 크기에 충분한 공간이 있는 데이터 저장소를 찾아 확인을 클릭하고 다음을 클릭합니다.
10. SCSI 가상 디바이스 노드를 선택한 후(기본 선택을 사용할 수 있음) 다음을 클릭합니다.

    선택한 노드는 *SCSI* 형식이어야 합니다. 다른 형식을 선택하면 *Panorama*가 부팅되지 않습니다.
11. 설정이 올바른지 확인한 다음 마침 및 확인을 클릭합니다.

    새 디스크가 가상 어플라이언스의 디바이스 목록에 나타납니다.
12. 필요한 경우 4단계에서 11단계를 반복하여 Panorama 가상 어플라이언스에 디스크를 추가합니다.
13. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고전원 > 전원 켜기를 선택합니다. 가상 디스크는 처음 사용을 위해 초기화됩니다. 새 디스크의 크기에 따라 초기화 시간이 결정됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048000MB ## : ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### # #####. #### ########.

STEP 3 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 4 | 로그를 수신하도록 Panorama를 구성합니다.

이 단계는 Panorama 모드에서 새로운 Panorama 배포를 위한 것입니다. 기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 5단계로 계속 진행합니다.

1. 관리형 수집기를 구성합니다.
2. 수집기 그룹을 구성합니다.
3. Panorama에 대한 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 수집기 그룹을 선택하고 Panorama 가상 어플라이언스가 속한 수집기 그룹을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

vCloud Air의 Panorama에 가상 디스크 추가

가상 로깅 디스크를 추가하여 Panorama™ 가상 어플라이언스에서 로그 스토리지 용량을 확장할 수 있습니다. 어플라이언스가 Panorama 모드인 경우 각각 2TB의 가상 로깅 디스크 1~12개 또는 최대 총 24TB까지 24TB 로깅 디스크 1개를 추가할 수 있습니다. 어플라이언스가 레거시 모드에 있는 경우 최대 8TB의 가상 로깅 디스크 하나를 추가할 수 있습니다.

*Panorama*에서 새 가상 디스크에 대한 연결이 끊어지면 *Panorama*에서 오류 기간 동안 로그가 손실될 수 있습니다.

필요한 경우 vCloud Air에서 가상 디스크를 교체할 수 있습니다.

STEP 1 | Panorama에 추가 디스크를 추가합니다.

모든 모드에서 *Panorama VM*의 첫 번째 로깅 디스크는 디스크를 추가하려면 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB* 미만인 경우 디스크 공간을 추가할 수 없습니다.

1. vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud On Demand** 지역을 선택합니다.
2. 가상 머신 탭에서 Panorama 가상 어플라이언스를 선택합니다.
3. 다른 디스크를 추가합니다(작업 > 리소스 편집).
4. 스토리지 크기를 설정합니다. Panorama 가상 어플라이언스가 Panorama 모드인 경우 크기를 2TB 이상으로 설정합니다. 디바이스가 레거시 모드인 경우 최대 8TB까지 크기를 설정할 수 있습니다.

   Panorama 모드에서는 *2TB*보다 큰 디스크 크기를 추가할 수 있으며 *Panorama*는 가능한 한 많은 *2TB* 파티션을 자동으로 생성합니다. 예를 들어 디스크 *sdc*가 *24TB*인 경우 *Panorama*는 *12*개의 *2TB* 파티션을 생성합니다. 이러한 디스크의 이름은 *sdc1*에서 *sdc12*까지 지정됩니다.
5. 스토리지 계층을 표준 또는 **SSD** 가속으로 설정합니다.
6. 필요에 따라 이전 단계를 반복하여 Panorama 가상 어플라이언스에 디스크를 추가합니다.
7. 변경 내용을 저장합니다.

STEP 2 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048000MB ## : ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답: ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 ## ### ### ## 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.

4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 3 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
3. 디스크를 선택하고 각각의 새 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.

6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 4 | 로그를 수신하도록 Panorama를 구성합니다.

이 단계는 Panorama 모드에서 새로운 Panorama 배포를 위한 것입니다. 기존 가상 Panorama 어플라이언스에 로깅 디스크를 추가하는 경우 다음 단계를 계속하십시오.

1. 관리형 수집기를 구성합니다.
2. 수집기 그룹을 구성합니다.
3. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 5 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 수집기 그룹을 선택하고 가상 Panorama 어플라이언스가 속한 수집기 그룹을 선택합니다.
3. 로그 스토리지 용량이 새 디스크 용량을 정확하게 표시하는지 확인하십시오.

Alibaba Cloud의 Panorama에 가상 디스크 추가

Alibaba Cloud에 Panorama 설치 이후에 가상 로깅 디스크를 추가하여 관리되는 방화벽에서 생성된 로그에 대한 Panorama™ 가상 어플라이언스의 로그 스토리지 용량을 확장합니다. Panorama 모드의

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스 또는 전용 로그 수집기에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. 가상 디스크를 추가하려면 Alibaba Cloud Console, Panorama 명령줄 인터페이스(CLI) 및 Panorama 웹 인터페이스에 대한 액세스 권한이 있어야 합니다.

Alibaba Cloud의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Alibaba Cloud Console에 로그인합니다.

STEP 2 | **Elastic Compute Service** > 인스턴스 **&** 이미지 > 인스턴스를 선택한 다음 Panorama 가상 어플라이언스 인스턴스로 이동합니다.

STEP 3 | Panorama에 가상 로깅 디스크를 추가합니다.



모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. 작업 열에서 관리를 선택합니다.
2. 클라우드 디스크 및 디스크 생성을 선택합니다.
3. 가상 로깅 디스크를 구성합니다.
   - 연결 - **ECS** 인스턴스에 연결을 선택합니다.
   - **ECS** 인스턴스 - 지역 및 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
   - 스토리지 - 가상 디스크 유형을 선택하고 디스크 용량을 입력합니다.
   - (선택 사항) 수량 - 생성할 가상 디스크 수를 지정합니다. 기본적으로 1개의 가상 디스크가 생성됩니다. 여러 로깅 디스크를 생성할 때 모든 가상 디스크의 합계가 24TB를 초과하지 않는지 확인하십시오.
   - 서비스 약관 - Alibaba Cloud 서비스 약관을 검토하고 검토한 후 확인하십시오.
4. 가상 디스크 생성을 미리 봅니다.
5. 새 가상 디스크를 생성합니다.

   새 가상 디스크를 생성하면 상태 창이 표시됩니다. 가상 디스크가 성공적으로 생성되면 디스크 목록으로 이동하여 디스크가 성공적으로 생성되었는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

   ```
   ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## # #
   ```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 ## ### ### ## 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 다음 단계를 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 5 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 6 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 6단계로 건너뜁니다.

1. 수집기 그룹 구성.
2. Panorama에 대한 로그 포워딩 구성.

STEP 7 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

AWS의 Panorama에 가상 디스크 추가

AWS 또는 AWS GovCloud에 Panorama 설치에 Panorama를 설치한 후 Panorama™ 가상 어플라이언스 인스턴스에 가상 로깅 디스크를 추가하여 관리형 방화벽에서 생성된 로그에 대한 스토리지를 제공합니다. Panorama 모드의 Panorama 가상 어플라이언스 또는 Dedicated Log Collector에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. 가상 디스크를 추가하려면 Amazon Web Service 콘솔, Panorama 명령줄 인터페이스(CLI) 및 Panorama 웹 인터페이스에 대한 액세스 권한이 있어야 합니다.

AWS의 Panorama 가상 어플라이언스는 2TB의 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | AWS Web Service 콘솔에 로그인하고 EC2 대시보드를 선택합니다.

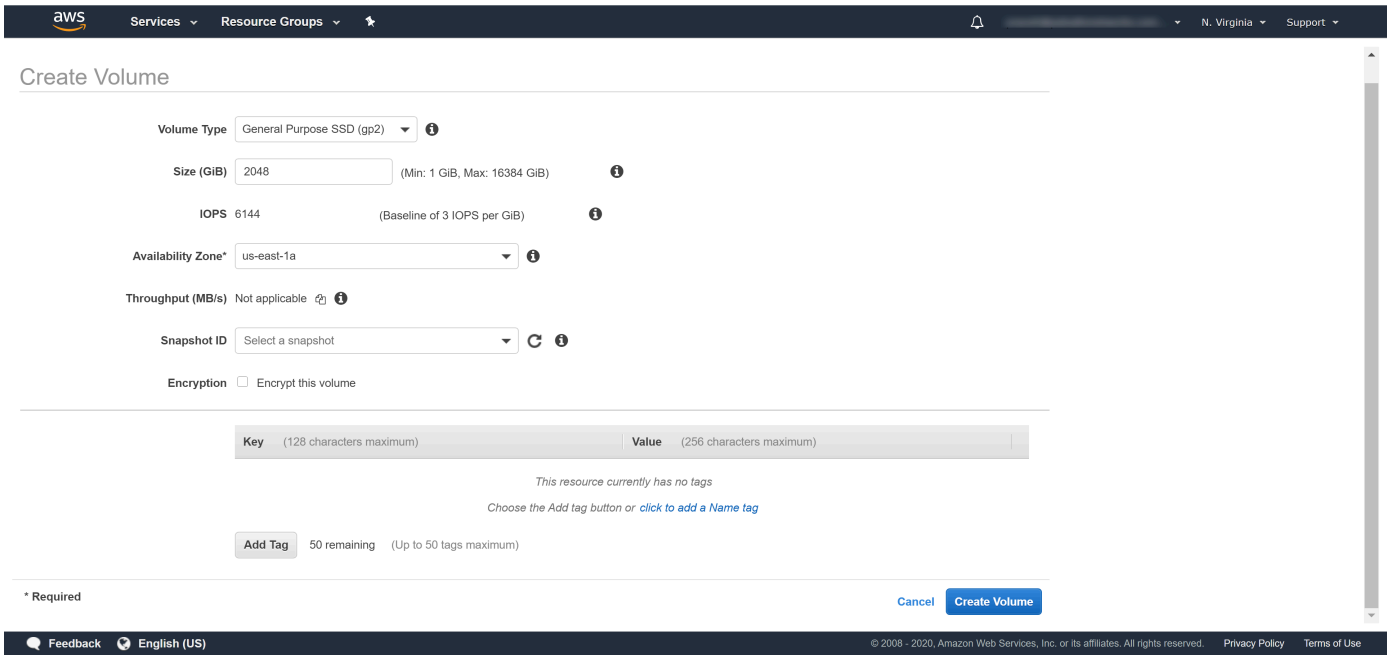
- Amazon Web Service Console
- AWS GovCloud 웹 서비스 콘솔

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에 가상 로깅 디스크를 추가합니다.

모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. EC2 대시보드에서 볼륨 및 볼륨 생성을 선택합니다.
   - 원하는 볼륨 유형을 선택합니다. 범용의 경우 범용 **SSD(GP2)**를 선택합니다.
   - 볼륨의 크기를 2048GiB로 구성합니다.
   - Panorama 가상 어플라이언스 인스턴스가 있는 동일한 가용 영역을 선택하십시오.
   - (선택 사항) 볼륨을 암호화합니다.
   - (선택 사항) 볼륨에 태그를 추가합니다.
2. 볼륨 생성을 클릭합니다.



3. Volumes 페이지에서 원하는 볼륨을 선택하고작업 > 볼륨 연결을 선택합니다.
4. Panorama 가상 어플라이언스 인스턴스를 연결합니다.
   1. Panorama 인스턴스를 선택합니다.
   2. 생성한 로깅 디스크 볼륨의 디바이스 이름을 지정합니다.

©2024 Palo Alto Networks, Inc.

STEP 3 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
## : nvme1n1 ## : ## ## : 2048000MB ## : ## ### ## : ### ### ##:
nvme2n1 ##: ## ## : 2048000MB ## : ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **nvme2n1**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을*(*를*)* 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.

4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 4 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.

6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 5 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 6단계로 건너뜁니다.

1. 수집기 그룹을 구성합니다.
2. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 6 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

©2024 Palo Alto Networks, Inc.

Azure의 Panorama에 가상 디스크 추가

Azure에 Panorama를 설치한 후 Panorama™ 가상 어플라이언스 인스턴스에 가상 로깅 디스크를 추가하여 관리되는 방화벽에서 생성된 로그에 대한 스토리지를 제공합니다. Panorama 모드의 Panorama 가상 어플라이언스 또는 Dedicated Log Collector에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. 가상 디스크를 추가하려면 Microsoft Azure Portal, Panorama CLI(명령줄 인터페이스) 및 Panorama 웹 인터페이스에 대한 액세스 권한이 있어야 합니다.

Azure의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스 파티션이 2TB 파티션에 디스크를 로깅하기 때문에 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

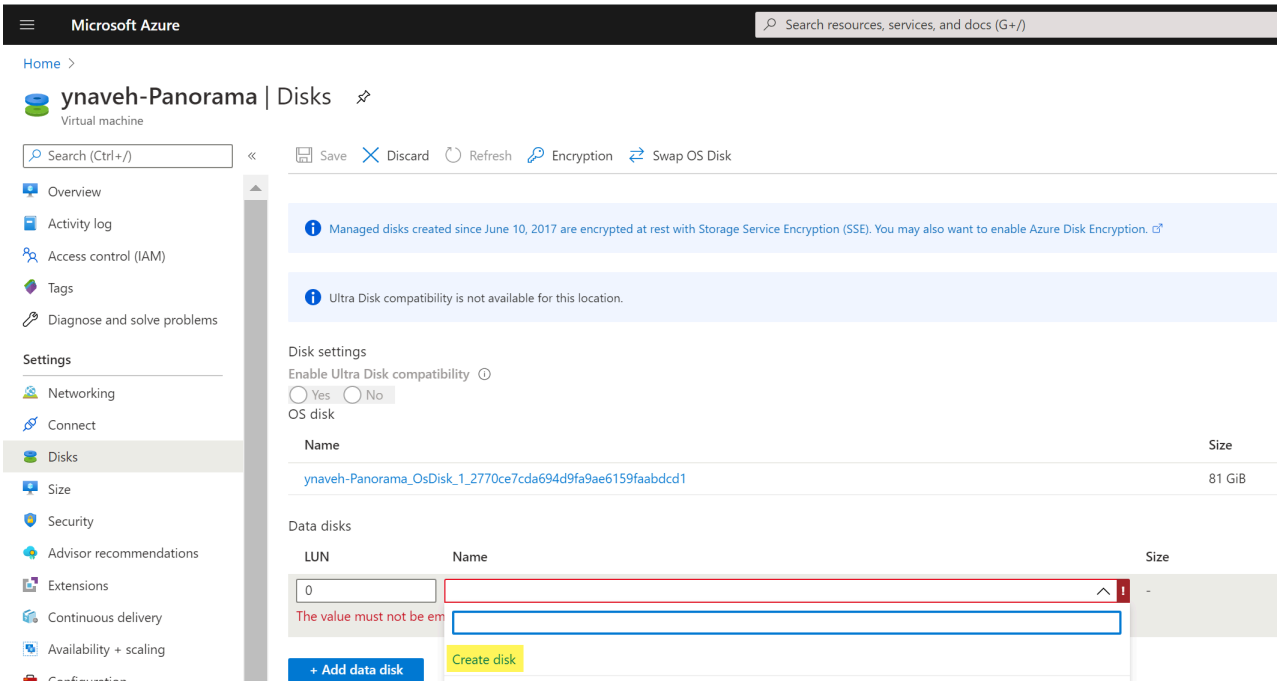
STEP 1 | Microsoft Azure 포털에 로그인합니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에 가상 로깅 디스크를 추가합니다.

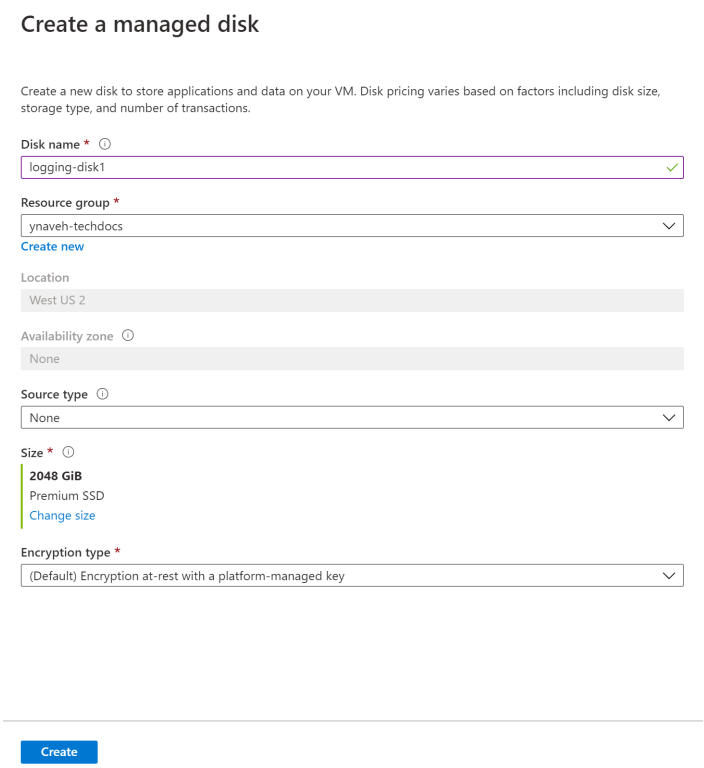
모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. Azure 대시보드에서 로깅 디스크를 추가할 Panorama 가상 머신을 선택합니다.
2. 디스크를 선택합니다.
3. +데이터 디스크를 추가합니다.
4. 새 디스크의 드롭다운에서 디스크 생성을 클릭합니다.



5. 로깅 디스크를 구성합니다.
   1. 디스크 이름을 입력합니다.
   2. 리소스 그룹을 선택합니다. 새 리소스 그룹을 만드는 경우 그룹 이름을 입력합니다.
   3. 계정 유형을 확인하십시오(이 필드는 자동으로 채워집니다).
   4. 소스 유형 드롭다운에서 없음을 선택합니다.
   5. 크기 변경을 선택하고 2048GiB 로깅 디스크를 선택합니다.
   6. 새 로깅 디스크를 생성합니다.

©2024 Palo Alto Networks, Inc.



7. 호스트 캐싱에 대해 읽기/쓰기를 선택합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 각 디스크를 활성화합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048000MB ## : ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을*(*를*)* 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 4 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집**Panorama** > 관리 수집기)
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 5 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 6단계로 건너뜁니다.

1. 수집기 그룹을 구성합니다.
2. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 6 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

©2024 Palo Alto Networks, Inc.

Google Cloud Platform의 Panorama에 가상 디스크 추가

Google Cloud Platform에 Panorama를 설치한 후 Panorama™ 가상 어플라이언스 인스턴스에 가상 로깅 디스크를 추가하여 관리형 방화벽에서 생성된 로그에 대한 스토리지를 제공합니다. Panorama 모드의 Panorama 가상 어플라이언스 또는 Dedicated Log Collector에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. Google Cloud Platform의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Google Cloud Console에 로그인합니다.

STEP 2 | 가상 로깅 디스크를 추가합니다.



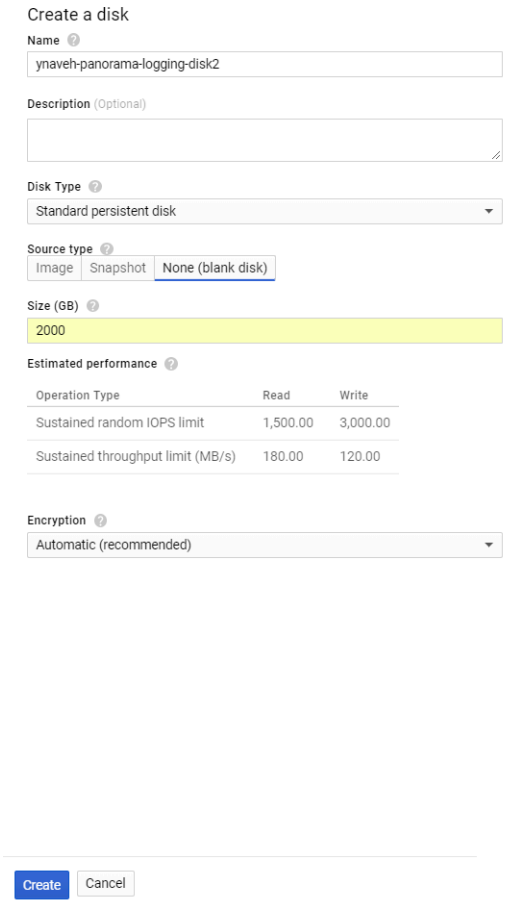
모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. 제품 및 서비스 메뉴에서 Panorama 가상 어플라이언스 인스턴스(**Compute Engine** > **VM** 인스턴스)를 선택한 다음 편집합니다.
2. 추가 디스크 섹션에서 항목을 추가합니다.
3. 디스크를 생성합니다(이름 드롭다운).

©2024 Palo Alto Networks, Inc.

STEP 3 | 가상 로깅 디스크를 구성합니다.

1. 이름을 입력합니다.
2. 디스크 유형 드롭다운 메뉴를 확장하고 원하는 유형을 선택합니다.
3. 소스 유형에 대해 없음**(**빈 디스크**)**을 선택합니다.
4. 가상 로깅 디스크의 크기**(GB)**를 설정합니다.
5. 생성을 클릭합니다.



6. Panorama 가상 어플라이언스 인스턴스를 업데이트하려면 변경 사항을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048000MB ## : ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 5 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 6 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 7단계로 건너뜁니다.

1. 수집기 그룹을 구성합니다.
2. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 7 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

©2024 Palo Alto Networks, Inc.

KVM의 Panorama에 가상 디스크 추가

KVM에 Panorama를 설치한 후 Panorama™ 가상 어플라이언스 인스턴스에 가상 로깅 디스크를 추가하여 관리되는 방화벽에서 생성된 로그에 대한 스토리지를 제공하십시오. Panorama 모드의 Panorama 가상 어플라이언스 또는 Dedicated Log Collector에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. KVM의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Virtual Machine Manager에서 Panorama 가상 어플라이언스 인스턴스를 종료합니다.

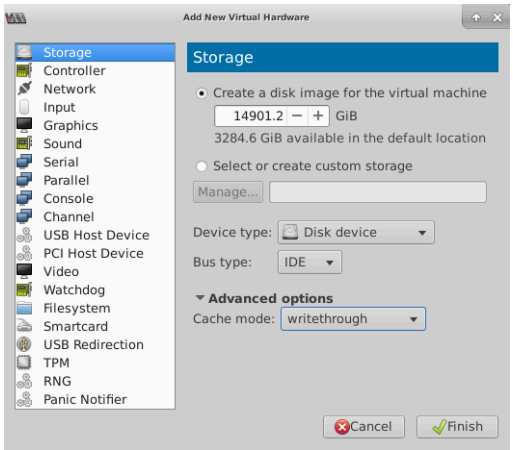
STEP 2 | Virtual Machine Manager에서 Panorama 가상 어플라이언스 인스턴스를 두 번 클릭하고 가상 하드웨어 세부 정보 표시를 클릭합니다.

STEP 3 | 가상 로깅 디스크를 추가합니다. 이 단계를 필요한 만큼 반복합니다.

모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. 가상 이미지에 대한 디스크 이미지를 생성하고(하드웨어 > 스토리지 추가) 가상 디스크 스토리지 용량을 적절한 2TB 값(Virtual Machine Manager에 따라 2000GB 또는 14901.2GiB)으로 구성합니다.

   버전에 따라 일부 *Virtual Machine Manager*는 *GiB*(기비바이트)를 사용하여 메모리를 할당합니다. 가상 로깅 디스크를 프로비저닝하지 않고 *Panorama* 가상 어플라이언스를 유지 관리 모드로 보내는 것을 방지하려면 필요한 스토리지 용량을 올바르게 변환해야 합니다.
2. 디바이스 유형 드롭다운에서 디스크 디바이스를 선택합니다.
3. 버스 유형 드롭다운에서 구성에 따라 **VirtIO** 또는 **IDE**를 선택합니다.
4. 고급 옵션을 확장하고 캐시 모드 드롭다운에서 연속 기입을 선택합니다.
5. 마침을 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama 가상 어플라이언스 인스턴스의 전원을 켭니다.

STEP 5 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048MB ##: ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 ## ### ### ## 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 6 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성(*HA*) 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 7 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 8단계로 건너뜁니다.

1. 수집기 그룹을 구성합니다.
2. Panorama에 대한 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

Hyper-V의 Panorama에 가상 디스크 추가

Hyper-V에 Panorama 설치 이후에 가상 로깅 디스크를 Panorama™ 가상 어플라이언스 인스턴스에 추가하여 관리형 방화벽에서 생성된 로그에 대한 스토리지를 제공합니다. Panorama 모드의 Panorama 가상 어플라이언스 또는 Dedicated Log Collector에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. Hyper-V의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Panorama 가상 어플라이언스의 전원을 끕니다.

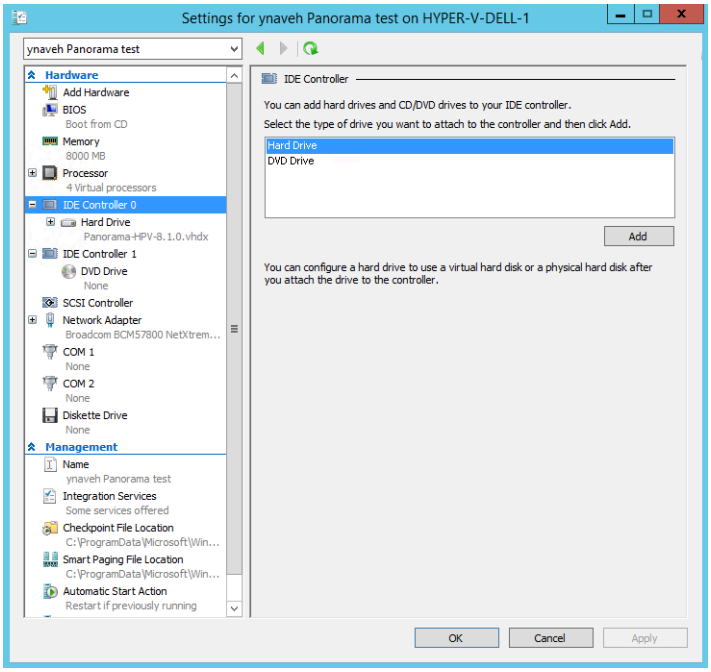
1. Hyper-V Manager의 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. 작업 > 끄기를 선택하여 Panorama 가상 어플라이언스의 전원을 끕니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | 가상 로깅 디스크를 추가합니다. 이 단계를 필요한 만큼 반복합니다.

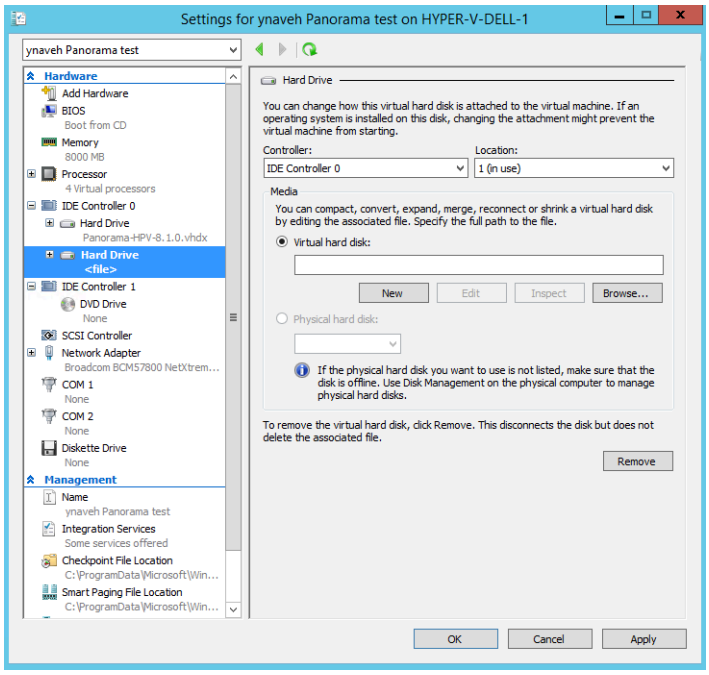
모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. **Virtual Machines** 목록에서 Panorama 가상 어플라이언스를 선택하고 작업 > 설정을 선택합니다.
2. 하드웨어 목록에서 **IDE** 컨트롤러 **0**을 선택합니다.
3. **IDE** 컨트롤러 드라이브 목록에서 하드 드라이브를 선택하고 새 가상 로깅 디스크를 추가합니다.



4. **IDE** 컨트롤러 **0**에서 생성된 새 하드 드라이브를 선택합니다.
5. 미디어에서 새 하드 디스크를 추가합니다.

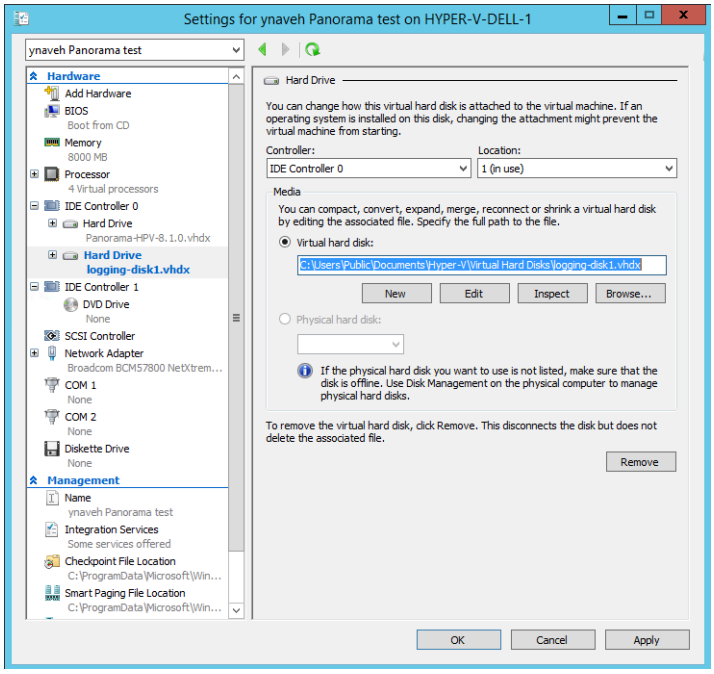
 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 새 가상 로깅 디스크를 구성합니다.

1. 시작하기 전에 프롬프트가 표시되면 다음을 클릭하여 가상 로깅 디스크 추가를 시작합니다.
2. 디스크 형식으로**VHDX**를 선택합니다. 계속하려면 다음을 클릭합니다.
3. 디스크 유형에 대해 필요에 따라 고정 크기 또는 동적 확장을 선택합니다. 계속하려면 다음을 클릭합니다.
4. 가상 로깅 디스크 파일의 이름과 위치를 지정합니다. 계속하려면 다음을 클릭합니다.
5. 디스크를 구성하려면 새 가상 하드 디스크 생성을 선택하고 디스크 크기를 입력합니다. 계속하려면 다음을 클릭합니다.
6. 요약을 검토하고 가상 하드 로깅 디스크 추가를 마칩니다.
7. 새 하드 디스크 추가를 적용합니다.



STEP 4 | Panorama 가상 어플라이언스의 전원을 켭니다.

1. 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. 작업 > 시작을 선택하여 Panorama 가상 어플라이언스의 전원을 켭니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

```
 ## : sdb ## : ## ## : 2048000MB ## : ## ### ## : ### ## ## : sdc #
# : ## ## : 2048MB ##: ## ### ## : ### ## # #
```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을(를) 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인하고 4단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 6 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 7 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 8단계로 건너뜁니다.

1. 수집기 그룹을 구성합니다.
2. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 8 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

Oracle Cloud Infrastructure(OCI)의 Panorama에 가상 디스크 추가

Oracle Cloud Infrastructure(OCI)에 Panorama 설치 이후에 가상 로깅 디스크를 추가하여 관리되는 방화벽에서 생성된 로그에 대한 Panorama™ 가상 어플라이언스의 로그 스토리지 용량을 확장합니다. Panorama 모드의 Panorama 가상 어플라이언스 또는 전용 로그 수집기에 대해 로컬 로그 수집기에 가상 디스크를 추가할 수 있습니다. 가상 디스크를 추가하려면 OCI 콘솔, Panorama 명령줄 인터페이스(CLI) 및 Panorama 웹 인터페이스에 대한 액세스 권한이 있어야 합니다.

OCI의 Panorama 가상 어플라이언스는 2TB 로깅 디스크만 지원하며 총 24TB의 로그 스토리지를 지원합니다. Panorama 가상 어플라이언스는 로깅 디스크를 2TB 파티션으로 분할하므로 2TB보다 작은 로깅 디스크 또는 2TB로 균등하게 나눌 수 없는 크기의 로깅 디스크를 추가할 수 없습니다. 예를 들어, 4TB 로깅 디스크를 연결하면 Panorama는 2개의 2TB 파티션을 생성합니다. 하지만 남은 1TB는 파티션으로 지원되지 않기 때문에 5TB 로깅 디스크를 추가할 수 없습니다.

STEP 1 | Oracle Cloud Infrastructure 콘솔에 로그인합니다.

STEP 2 | 2TB 블록 볼륨을 생성합니다.

1. 블록 스토리지 > 블록 볼륨 및 블록 볼륨 생성을 선택합니다.
2. 볼륨에 대한 설명이 포함된 이름을 입력합니다.
3. Panorama 가상 어플라이언스 인스턴스와 동일한 가용성 도메인을 선택하십시오.
4. 사용자 정의 볼륨 크기를 선택하십시오.
5. 볼륨 크기에 **2000**을 입력합니다.
6. 블록 볼륨을 생성합니다.

STEP 3 | 가상 로깅 디스크를 Panorama 가상 어플라이언스 인스턴스에 연결합니다.

모든 모드에서 추가 디스크를 추가하려면 *Panorama VM*의 첫 번째 로깅 디스크가 *2TB* 이상이어야 합니다. 첫 번째 로깅 디스크가 *2TB*보다 작으면 추가 디스크 공간을 추가할 수 없습니다.

1. **Compute** > **Instances**를 선택한 다음 Panorama 가상 어플라이언스 인스턴스의 이름을 클릭합니다.
2. 리소스에서 **Attached Block Volumes** 및 **Attach Block Volume**을 선택합니다.
3. 볼륨의 경우 볼륨을 선택하고 가상 로깅 디스크를 선택합니다.
4. 첨부 파일 유형으로 반가상화를 선택합니다.
   이는 Panorama 가상 어플라이언스가 가상 로깅 디스크를 인식하기 위해 필요합니다.
5. 액세스에 대해 읽기/쓰기를 선택합니다.
6. 가상 로깅 디스크를 연결합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | 각 디스크를 구성합니다.

다음 예에서는 sdc 가상 디스크를 사용합니다.

1. Panorama CLI에 로그인.
2. Panorama 가상 어플라이언스에서 디스크를 보려면 다음 명령을 입력하십시오.
   ### ### ## ## ##

   사용자에게 다음 응답이 표시됩니다.

   ```
   ## : sdb ## : ## ## : 2048000MB ## : ### # ## ##: ### ## # #
   ```

3. 다음 명령을 입력하고 ### ## ## #### ## #### #### ### #####. ### #### 응답:
   ## ### ### ## **sdc**

   이 모드에서는 로깅이 지원되지 않으므로 *## ### ### ##* 명령은 관리 전용 모드의 *Panorama* 관리 서버에서 사용할 수 없습니다. 명령이 표시되지 않으면 로깅 디스크를 활성화하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스 설정을*(*를*)* 수행합니다. *Panorama* 모드에서 Panorama CLI에 로그인을*(*를*)* 수행하고 다음 단계로 계속 진행하여 디스크 추가를 확인합니다.
4. ### ### #### ## 명령을 입력하여 디스크 추가 상태를 확인합니다. 새로 추가된 모든 디스크 응답에 ### #### ## ### #####. #### ########.

STEP 5 | 로깅에 사용할 수 있는 디스크를 생성합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. 로그 수집기 편집(**Panorama** > 관리 수집기).
3. 디스크를 선택하고 새로 추가된 각 디스크를 추가합니다.
4. 확인을 클릭합니다.
5. 커밋 > **Panorama**에 커밋을 선택합니다.

   능동/수동 고가용성*(HA)* 구성의 *Panorama*의 경우 계속하기 전에 *HA* 동기화가 완료될 때까지 기다리십시오.
6. 커밋 > 디바이스에 푸시를 선택하고 Log Collector가 속한 Collector Group에 변경 사항을 푸시합니다.

STEP 6 | (Panorama 모드의 새 Panorama 배포만 해당) 로그를 수신하도록 Panorama를 구성합니다.

기존 Panorama 가상 어플라이언스에 로깅 디스크를 추가하는 경우 6단계로 건너뜁니다.

1. 수집기 그룹 구성.
2. Panorama에 대한 로그 포워딩 구성.

STEP 7 | Panorama Log Storage 용량이 증가했는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. Panorama 가상 어플라이언스가 속한 수집기 그룹(**Panorama** > 수집기 그룹)을 선택합니다.
3. 로그 스토리지 용량이 디스크 용량을 정확하게 표시하는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

NFS 데이터 저장소에 Panorama ESXi 서버 탑재

레거시 모드의 Panorama 가상 어플라이언스가 ESXi 서버에서 실행되는 경우 NFS(네트워크 파일 시스템) 데이터 저장소에 탑재하면 중앙 집중식 위치에 로깅하고 가상 디스크가 지원하는 것 이상으로 로그 스토리지 용량을 확장할 수 있습니다. (ESXi 5.5 이상의 버전은 최대 8TB의 가상 디스크를 지원할 수 있습니다. 이전 ESXi 버전은 최대 2TB의 가상 디스크를 지원합니다.) Panorama 고가용성(HA) 구성에서 NFS 데이터 저장소를 설정하기 전에 Panorama HA의 로깅 고려 사항을(를) 참조하십시오.

Panorama 모드의 *Panorama* 가상 어플라이언스는 *NFS*를 지원하지 않습니다.

STEP 1 | **Panorama** > 설정 > 작업를 선택한 다음 기타 섹션에서 스토리지 파티션 설정을 클릭합니다.

STEP 2 | 스토리지 파티션 유형을 **NFS V3**으로 설정합니다.

STEP 3 | NFS 서버의 IP 주소를 입력합니다.

STEP 4 | 로그 파일을 저장할 로그 디렉토리 경로를 입력합니다. 예를 들어, export/panorama입니다.

STEP 5 | 프로토콜에서 **TCP** 또는 **UDP**를 선택한 다음 NFS 서버에 액세스하기 위한 포트를 입력합니다.

*TCP*를 통한 *NFS*를 사용하려면 *NFS* 서버가 이를 지원해야 합니다. 일반적인 *NFS* 포트는 *RPC*의 경우 *UDP/TCP 111*이고 *NFS*의 경우 *UDP/TCP 2049*입니다.

STEP 6 | 최적의 NFS 성능을 위해 읽기 크기 및 쓰기 크기 필드에서 클라이언트와 서버가 서로 주고받는 데이터 청크의 최대 크기를 지정합니다. 읽기/쓰기 크기를 정의하면 Panorama와 NFS 데이터 저장소 간에 데이터를 전송할 때 데이터 볼륨과 속도가 최적화됩니다.

STEP 7 | (선택 사항) 설정 시 복사를 선택하여 Panorama에 저장된 기존 로그를 NFS 볼륨으로 복사합니다. Panorama에 많은 로그가 있는 경우 이 옵션은 대용량 데이터 전송을 시작할 수 있습니다.

STEP 8 | Panorama가 NFS 서버 및 로그 디렉토리에 액세스할 수 있는지 확인하려면 로깅 파티션 테스트를 클릭합니다.

STEP 9 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 10 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다. 다시 부팅할 때까지 Panorama 가상 어플라이언스는 로컬 스토리지 디스크에 로그를 씁니다.

STEP 11 | **Panorama** > 설정 > 작업를 선택한 다음 디바이스 작업 섹션에서 **Panorama** 재부팅을 선택합니다. 재부팅 후 Panorama는 NFS 데이터스토어에 로그를 쓰기 시작합니다.

Panorama 가상 어플라이언스에서 CPU 및 메모리 늘리기

Panorama 가상 어플라이언스의 초기 구성을 수행할 때 어플라이언스가 Panorama 모드인지 관리 전용 모드인지의 여부와 로그 스토리지 용량 또는 관리되는 방화벽 수를 기반으로 메모리와 CPU 수를 지정합니다. 나중에 스토리지 용량이나 관리되는 방화벽을 추가하는 경우 메모리와 CPU도 늘려야 합니다. Log Collector 모드의 Panorama 가상 어플라이언스는 시스템 요구 사항을 충족해야 하며 CPU 및 메모리를 최소 요구 사항 이상으로 늘릴 필요가 없습니다. 각 Panorama 모드의 CPU 및 메모리 요구 사항에 대한 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토합니다.

 ©2024 Palo Alto Networks, Inc.

- ESXi 서버에서 Panorama용 CPU 및 메모리 늘리기
- vCloud Air에서 Panorama의 CPU 및 메모리 늘리기
- Alibaba Cloud에서 Panorama용 CPU 및 메모리 증가
- Panorama on AWS의 CPU 및 메모리 증가
- Azure에서 Panorama의 CPU 및 메모리 늘리기
- Google Cloud Platform에서 Panorama용 CPU 및 메모리 늘리기
- KVM에서 Panorama를 위한 CPU 및 메모리 늘리기
- Hyper-V에서 Panorama를 위한 CPU 및 메모리 늘리기
- Oracle Cloud Infrastructure(OCI)에서 Panorama의 CPU 및 메모리 늘리기

ESXi 서버에서 Panorama용 CPU 및 메모리 늘리기

Panorama에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스에서 CPU 및 메모리 늘리기을(를) 참조하십시오.

STEP 1 | VMware vSphere Client에 액세스하고 가상 머신을 선택합니다.

STEP 2 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.

STEP 3 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다.

STEP 4 | 메모리를 선택하고 새 메모리 크기를 입력합니다.

STEP 5 | **CPU**를 선택한 다음 CPU 수(가상 소켓 수에 소켓당 코어 수를 곱한 값)를 지정합니다.

STEP 6 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 7 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다.

vCloud Air에서 Panorama의 CPU 및 메모리 늘리기

Panorama에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스에서 CPU 및 메모리 늘리기을(를) 참조하십시오.

STEP 1 | vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud OnDemand** 지역을 선택합니다.

STEP 2 | 가상 머신 탭에서 Panorama 가상 머신을 선택한 다음 전원을 끕니다.

STEP 3 | 작업 > 리소스 편집을 선택합니다.

STEP 4 | **CPU** 및 메모리를 설정합니다.

STEP 5 | 변경 내용을 저장합니다.

STEP 6 | Panorama 가상 머신을 선택한 다음 전원을 켭니다.

 ©2024 Palo Alto Networks, Inc.

Alibaba Cloud에서 Panorama용 CPU 및 메모리 증가

Panorama™ 가상 어플라이언스의 인스턴스 유형을 변경하여 Panorama 가상 어플라이언스 인스턴스에 할당된 CPU 및 메모리를 늘릴 수 있습니다. 지원되는 Alibaba Cloud 인스턴스 유형을 검토하고 인스턴스 유형을 변경하기 전에 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 확인하십시오.

STEP 1 | Alibaba Cloud Console에 로그인합니다.

STEP 2 | **Elastic Compute Service** > 인스턴스 **&** 이미지 > 인스턴스를 선택한 다음 Panorama 가상 어플라이언스 인스턴스로 이동합니다.

STEP 3 | 작업 열에서 추가 > 인스턴스 상태 > 중지를 선택합니다.

STEP 4 | Panorama 가상 어플라이언스 인스턴스 유형을 변경합니다.

1. 아직 선택하지 않은 경우 Panorama 가상 어플라이언스를 선택합니다.
2. 작업 열에서 인스턴스 유형 변경을 선택합니다.
3. 원하는 인스턴스 유형을 선택한 다음 인스턴스 유형을 변경합니다.
4. 메시지가 표시되면 콘솔을 선택하여 Panorama 가상 어플라이언스 인스턴스를 봅니다.

STEP 5 | Panorama 가상 어플라이언스 인스턴스의 작업 열에서 추가 > 인스턴스 상태 > 시작을 선택합니다.

STEP 6 | 증가된 CPU 및 메모리를 확인합니다.

1. Panorama CLI에 로그인.
2. Panorma 가상 어플라이언스 시스템 정보를 봅니다.

```
admin> show system info
```

3. `num-cpus` 및 `ram-in-gb`에 선택한 인스턴스 유형에 따라 올바른 CPU 수와 메모리 양이 표시되는지 확인합니다.

Panorama on AWS의 CPU 및 메모리 증가

Panorama™에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스의 CPU 및 메모리 늘리기를 참조하십시오.

STEP 1 | AWS Web Service 콘솔에 로그인하고 EC2 대시보드를 선택합니다.

- Amazon Web Service Console
- AWS GovCloud 웹 서비스 콘솔

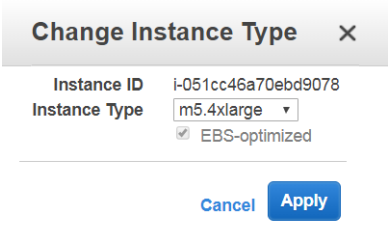
STEP 2 | EC2 대시보드에서 인스턴스를 선택한 다음 Panorama 가상 어플라이언스 인스턴스를 선택합니다.

STEP 3 | 작업 > 인스턴스 상태 > 중지를 선택하여 Panorama 가상 어플라이언스 인스턴스의 전원을 끕니다.

STEP 4 | 작업 > 인스턴스 설정 > 변경 인스턴스 유형을 선택하여 Panorama 가상 어플라이언스 인스턴스 유형을 변경합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 업그레이드할 인스턴스 유형을 선택한 다음 적용합니다.



STEP 6 | 작업 > 인스턴스 상태 > 시작을 선택하여 Panorama 가상 어플라이언스 인스턴스의 전원을 켭니다.

Azure에서 Panorama의 CPU 및 메모리 늘리기

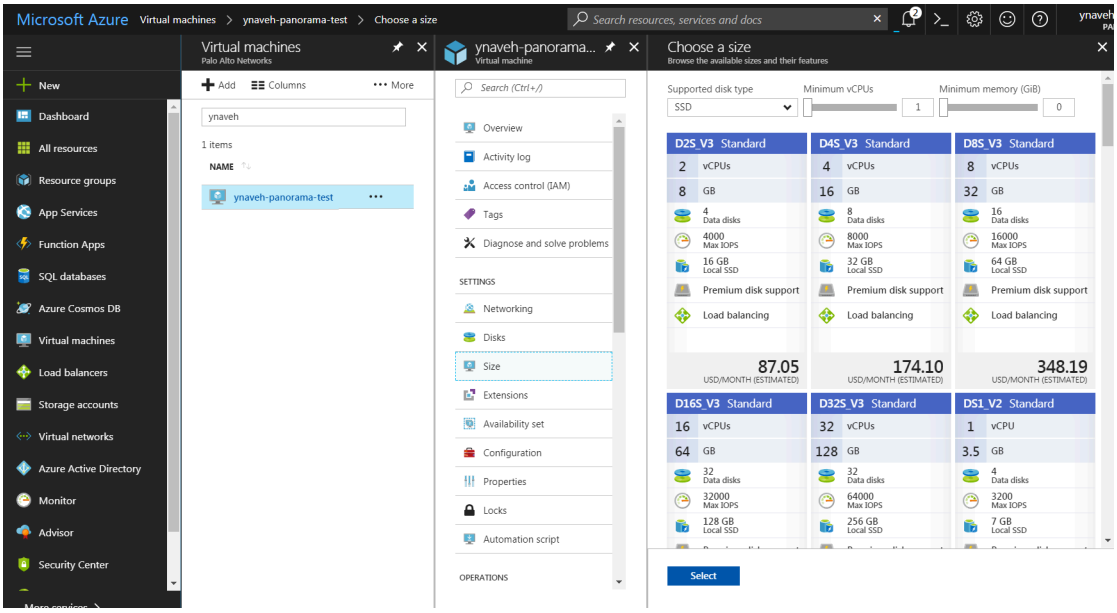
Panorama™에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스의 CPU 및 메모리 늘리기를 참조하십시오.

STEP 1 | Microsoft Azure 포털에 로그인합니다.

STEP 2 | Azure 대시보드의 가상 머신에서 Panorama 가상 어플라이언스를 선택합니다.

STEP 3 | 개요를 선택한 다음 Panorama 가상 어플라이언스를 중지합니다.

STEP 4 | 새 가상 머신 크기를 선택한 다음 선택합니다.



STEP 5 | 개요를 선택한 다음 Panorama 가상 어플라이언스를 시작합니다.

Google Cloud Platform에서 Panorama용 CPU 및 메모리 늘리기

Panorama™에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스의 CPU 및 메모리 늘리기를 참조하십시오.

STEP 1 | Google Cloud Console에 로그인합니다.

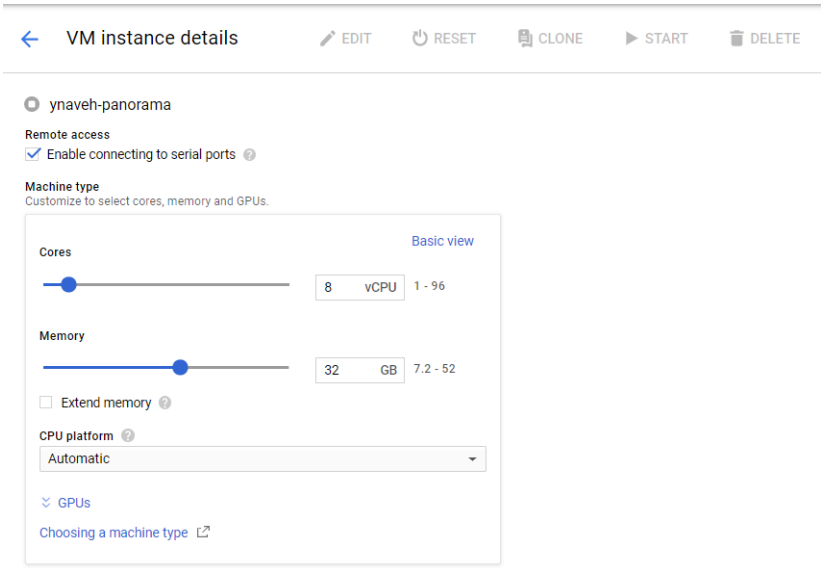
©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama 가상 어플라이언스 인스턴스를 중지합니다.

1. 제품 및 서비스 메뉴(**Compute Engine** > **VM** 인스턴스)에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. Panorama 가상 어플라이언스 인스턴스를 중지합니다. Panorama 가상 어플라이언스가 완전히 종료되는 데 2~3분이 소요될 수 있습니다.

STEP 3 | Panorama 가상 어플라이언스 리소스를 재구성합니다.

1. Panorama 가상 어플라이언스 인스턴스 세부정보를 편집합니다.
2. 머신 유형에서 Panorama 가상 어플라이언스 CPU 코어 및 메모리를 사용자 지정합니다.



STEP 4 | Panorama 가상 어플라이언스 인스턴스를 업데이트하려면 변경 사항을 저장합니다.

STEP 5 | Panorama 가상 어플라이언스를 시작합니다.

KVM에서 Panorama를 위한 CPU 및 메모리 늘리기

Panorama™에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스의 CPU 및 메모리 늘리기를 참조하십시오.

STEP 1 | Virtual Machine Manager에서 Panorama 가상 어플라이언스 인스턴스를 종료합니다.

STEP 2 | Virtual Machine Manager에서 Panorama 가상 어플라이언스 인스턴스를 두 번 클릭하고 가상 하드웨어 세부 정보 표시를 클릭합니다.

STEP 3 | 할당된 Panorama 가상 어플라이언스 CPU 코어를 편집합니다.

1. 현재 할당된 **CPU**를 편집합니다.
2. 재구성된 CPU 코어 할당을 적용합니다.

STEP 4 | 할당된 Panorama 가상 어플라이언스 메모리를 편집합니다.

1. 현재 할당된 메모리를 편집합니다.
2. 재구성된 메모리 할당을 적용합니다.

 ©2024 Palo Alto Networks, Inc.

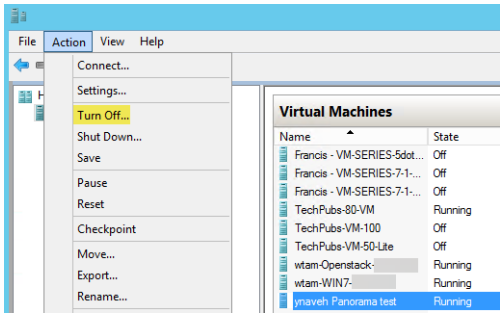
STEP 5 | Panorama 가상 어플라이언스 인스턴스의 전원을 켭니다.

Hyper-V에서 Panorama를 위한 CPU 및 메모리 늘리기

Panorama™에 필요한 최소 CPU 및 메모리는 Panorama 가상 어플라이언스의 CPU 및 메모리 늘리기를 참조하십시오.

STEP 1 | Panorama 가상 어플라이언스의 전원을 끕니다.

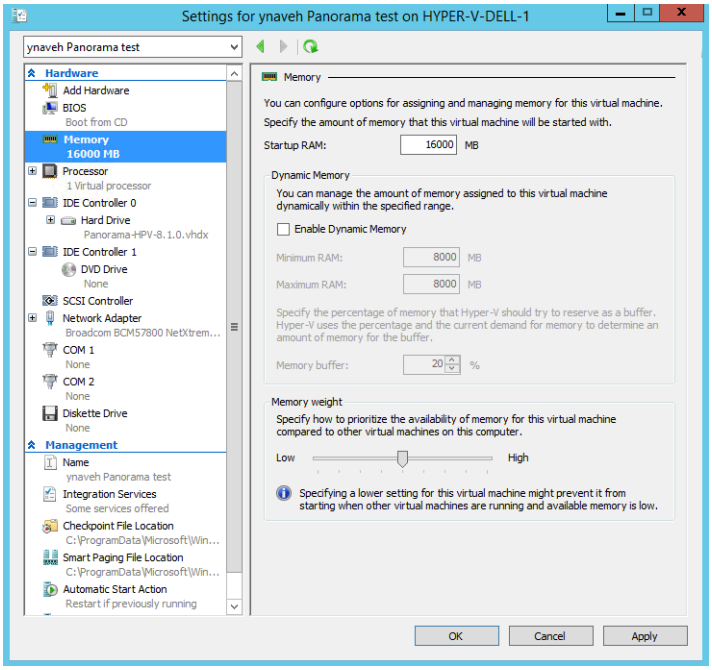
1. Hyper-V Manager의 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. 작업 > 끄기를 선택하여 Panorama 가상 어플라이언스의 전원을 끕니다.



STEP 2 | Hyper-V Manager에서 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택한 다음 작업 > 설정를 선택하여 Panorama 가상 어플라이언스 리소스를 편집합니다.

STEP 3 | 할당된 Panorama 가상 어플라이언스 메모리를 편집합니다.

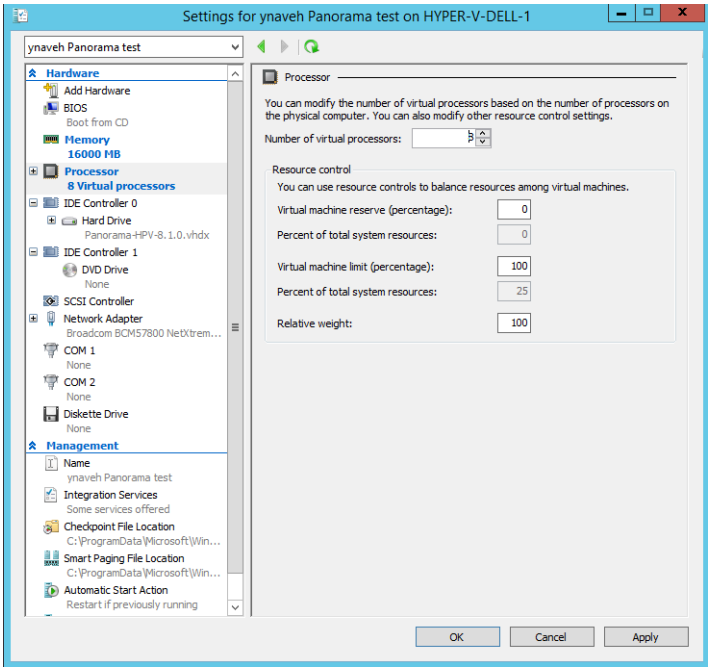
1. 하드웨어 목록에서 메모리를 선택합니다.
2. 현재 할당된 시작 **RAM**을 편집합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | 할당된 Panorama 가상 어플라이언스 CPU 코어를 편집합니다.

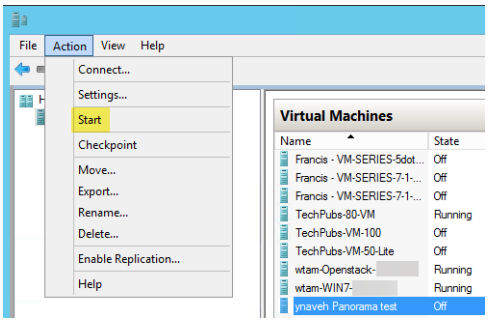
1. 하드웨어 목록에서 프로세서를 선택합니다.
2. 현재 할당된 가상 프로세서 수를 편집합니다.



STEP 5 | 재할당된 메모리와 CPU 코어를 적용합니다.

STEP 6 | Panorama 가상 어플라이언스의 전원을 켭니다.

1. 가상 머신 목록에서 Panorama 가상 어플라이언스 인스턴스를 선택합니다.
2. 작업 > 시작을 선택하여 Panorama 가상 어플라이언스의 전원을 켭니다.



Oracle Cloud Infrastructure(OCI)에서 Panorama의 CPU 및 메모리 늘리기

Panorama™ 가상 어플라이언스의 인스턴스 유형을 변경하여 Panorama 가상 어플라이언스 인스턴스에 할당된 CPU 및 메모리를 늘릴 수 있습니다. Panorama 가상 어플라이언스 인스턴스 CPU 및 메모리를 수정하기 전에 반드시 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토하십시오.

STEP 1 | Oracle Cloud Infrastructure 콘솔에 로그인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama 가상 어플라이언스 인스턴스의 전원을 끕니다.

1. **Compute** > **Instances**를 선택한 다음 Panorama 가상 어플라이언스 인스턴스의 이름을 클릭합니다.
2. Panorama 가상 어플라이언스 인스턴스를 중지합니다.

STEP 3 | CPU와 메모리를 늘립니다.

1. 인스턴스 세부 정보에서 편집 모양 > 편집을 선택합니다.
2. 인스턴스에 할당된 CPU 및 메모리 수를 늘립니다.
3. 변경 사항을 저장합니다.

STEP 4 | 인스턴스 세부 정보에서 Panorama 가상 어플라이언스를 시작합니다.

STEP 5 | 증가된 CPU 및 메모리를 확인합니다.

1. Panorama CLI에 로그인.
2. Panorma 가상 어플라이언스 시스템 정보를 봅니다.

```
admin> show system info
```

3. `num-cpus` 및 `ram-in-gb`에 선택한 인스턴스 유형에 따라 올바른 CPU 수와 메모리 양이 표시되는지 확인합니다.

Panorama 가상 어플라이언스의 시스템 디스크 늘리기

대규모 방화벽 배포 관리을(를) 할 때 Panorama 가상 어플라이언스가 대용량 데이터 세트를 지원하도록 시스템 디스크 용량을 224GB로 확장하면 동적 업데이트와 같은 작업을 위한 충분한 디스크 공간을 확보할 수 있습니다. 또한 224GB 시스템 디스크는 SD-WAN 배포를 관리하기 위해 Panorama 모드에서 Panorama 가상 어플라이언스를 사용하려는 경우 관리 방화벽 상태에 대한 데이터 모니터링 및 보고를 위해 스토리지를 확장합니다.

- ESXi 서버에서 Panorama용 시스템 디스크 늘리기
- Google Cloud Platform에서 Panorama용 시스템 디스크 늘리기

ESXi 서버에서 Panorama용 시스템 디스크 늘리기

기본 81GB 시스템 디스크를 교체하려면 224GB 시스템 디스크를 추가하십시오. Panorama 가상 어플라이언스의 최소 리소스 요구 사항은 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.

Panorama 가상 어플라이언스 시스템 디스크를 다시 *81GB*로 줄이는 것은 지원되지 않습니다.

STEP 1 | (모범 사례) Panorama 및 방화벽 구성 저장 및 내보내기.

문제가 발생할 경우 Panorama를 복구할 수 있도록 Panorama 및 방화벽 구성을 저장하고 내보내십시오.

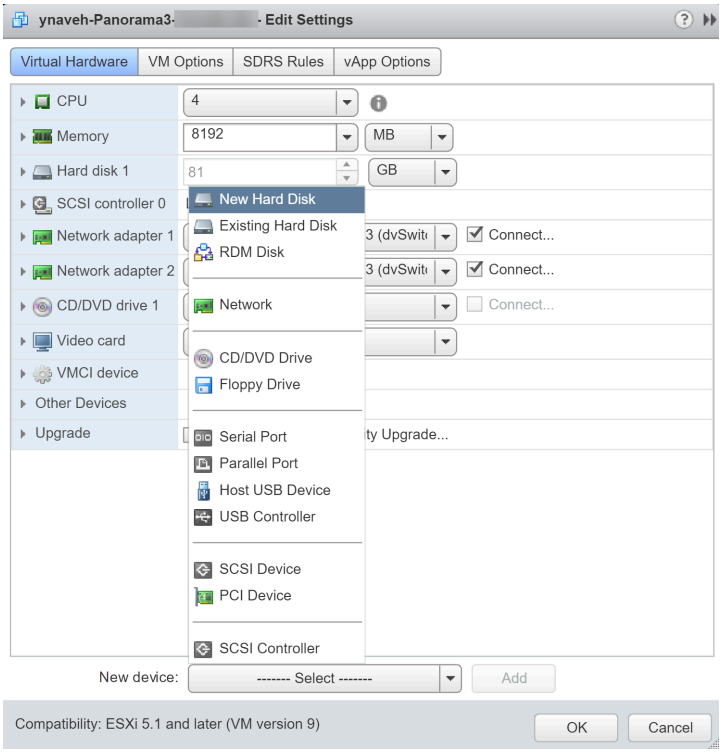
STEP 2 | VMware vSphere Client에 액세스하고 Panorama 가상 어플라이언스로 이동합니다.

STEP 3 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 새 224GB 시스템 디스크를 추가합니다.

1. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
2. 새 디바이스로 새 하드 디스크를 선택한 다음 새 디바이스를 추가합니다.
3. 새 하드 디스크를 224GB로 구성하고 확인을 클릭합니다.



STEP 5 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다.

*Panorama*에서 새 시스템 디스크를 초기화하는 데 최대 *30*분이 소요될 수 있습니다. 이 시간 동안 *Panorama* 웹 인터페이스와 *CLI*를 사용할 수 없습니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 이전 시스템 디스크에서 새 시스템 디스크로 디스크 데이터를 마이그레이션합니다.

이 예에서는 sdb라는 레이블이 붙은 새로 추가된 시스템 디스크로 마이그레이션합니다.

1. Panorama CLI에 로그인.
2. 마이그레이션에 사용 가능한 시스템 디스크를 보려면 다음 명령을 입력하십시오.

```
admin> request system clone-system-disk target ?
```

3. 다음 명령을 사용하여 디스크 데이터를 새 시스템 디스크로 마이그레이션합니다.

```
admin> request system clone-system-disk target sdb
```

디스크 마이그레이션을 시작하라는 메시지가 표시되면 **Y**를 입력합니다.

> 마이그레이션을 시작하기 위해 *Panorama*가 재부팅되고 디스크 마이그레이션을 완료하는 데 최소 *20*분이 걸립니다. 이 시간 동안 *Panorama* 웹 인터페이스와 *CLI*를 사용할 수 없습니다.

4. 웹 콘솔에서 디스크 마이그레이션을 모니터링합니다. Panorama가 디스크 마이그레이션이 완료되었음을 나타내는 다음 메시지를 표시한 후에만 다음 단계를 계속하십시오.

```
==================================
Disk Cloning Utility (Version 1.0)
==================================
SOURCE - Disk sda (82944 MB)
TARGET - Disk sdb (229376 MB)

Gathering disks info
Finished gathering disks info

Preparing disks
Finished preparing disks

Copying data
Finished copying data

Making disk bootable
Finished making disk bootable

Disk cloning procedure completed. Please shutdown the sytem and switch disks..._
```

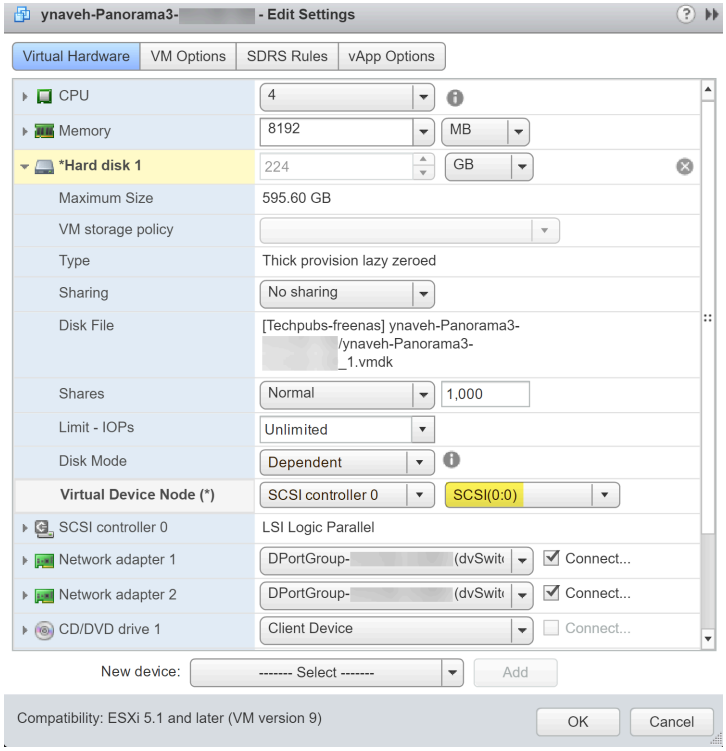
STEP 7 | 이전 시스템 디스크를 삭제합니다.

1. VMware vSphere Client에 액세스하고 Panorama 가상 어플라이언스로 이동합니다.
2. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.
3. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 클릭합니다.
4. 이전 81GB 시스템 디스크를 삭제하고 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 새 시스템 디스크의 가상 디바이스 노드를 수정합니다.

1. 새 시스템 디스크에 대한 설정 옵션을 확장합니다.
2. 가상 디바이스 노드로 **SCSI(0:0)**를 선택합니다.
3. 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 9 | Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다.

STEP 10 | 새 시스템 디스크로 성공적으로 마이그레이션되었는지 확인합니다.

1. Panorama CLI에 로그인.
2. 다음 명령을 입력하여 시스템 디스크 파티션을 봅니다.

   디스크 크기가 증가했는지 확인하려면 `/dev/root`, `/dev/sda5`, `/dev/sda6`, `/dev/sda8` 파티션을 확인해야 합니다.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

 ©2024 Palo Alto Networks, Inc.

Google Cloud Platform에서 Panorama용 시스템 디스크 늘리기

기본 81GB 시스템 디스크를 교체하려면 224GB 시스템 디스크를 추가하십시오. Panorama 가상 어플라이언스의 최소 리소스 요구 사항은 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.

STEP 1 | (모범 사례) Panorama 및 방화벽 구성 저장 및 내보내기.

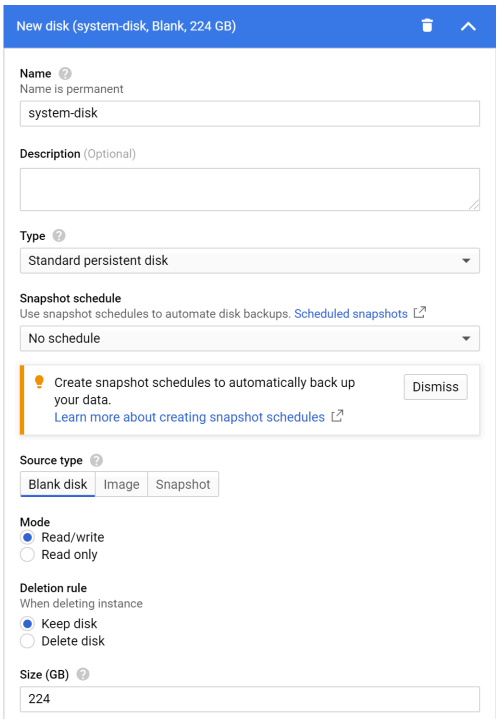
문제가 발생할 경우 Panorama를 복구할 수 있도록 Panorama 및 방화벽 구성을 저장하고 내보내십시오.

STEP 2 | Google Cloud Console에 로그인합니다.

STEP 3 | **VM** 인스턴스에서 Panorama VM 인스턴스를 중지합니다.

STEP 4 | 새 224GB 시스템 디스크를 추가합니다.

1. Panorama VM 인스턴스를 선택하고 편집을 선택합니다.
2. 추가 디스크 섹션에서 새 디스크를 추가합니다.
3. 224GB로 새 디스크를 구성하고 확인을 클릭합니다.



STEP 5 | **VM** 인스턴스에서 Panorama VM 인스턴스를 시작합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 이전 시스템 디스크에서 새 시스템 디스크로 디스크 데이터를 마이그레이션합니다.

이 예에서는 sdb라는 레이블이 붙은 새로 추가된 시스템 디스크로 마이그레이션합니다.

1. Panorama CLI에 로그인.
2. 마이그레이션에 사용 가능한 시스템 디스크를 보려면 다음 명령을 입력하십시오.

```
admin> request system clone-system-disk target ?
```

3. 다음 명령을 사용하여 디스크 데이터를 새 시스템 디스크로 마이그레이션합니다.

```
admin> request system clone-system-disk target sdb
```

디스크 마이그레이션을 시작하라는 메시지가 표시되면 **Y**를 입력합니다.

마이그레이션을 시작하기 위해 *Panorama*가 재부팅되고 디스크 마이그레이션을 완료하는 데 최소 *20*분이 걸립니다. 이 시간 동안 *Panorama* 웹 인터페이스와 *CLI*를 사용할 수 없습니다.

4. Panorama CLI에 로그인을 시도하여 디스크 마이그레이션을 모니터링합니다. Panorama 관리 서버는 시스템 디스크 마이그레이션이 완료된 후 유지 관리 모드에 있으며 유지 관리 모드에 있는 동안 Panorama CLI에 로그인할 수 있습니다.

STEP 7 | 새 224GB 시스템 디스크를 연결합니다.

1. **VM** 인스턴스에서 Panorama VM 인스턴스를 중지합니다.
2. Panorama VM 인스턴스를 선택하고 편집을 선택합니다.
3. 추가 디스크섹션에서 새 224GB 시스템 디스크를 분리합니다.
4. 부팅 디스크섹션에서 이전 81GB 시스템 디스크를 분리합니다.
5. 부팅 디스크 섹션에서 항목을 추가하고 새 224GB 시스템 디스크를 선택합니다.
6. 구성 변경 내용을 저장합니다.

STEP 8 | **VM** 인스턴스에서 Panorama VM 인스턴스를 시작합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 새 시스템 디스크로 성공적으로 마이그레이션되었는지 확인합니다.

1. Panorama CLI에 로그인.
2. 다음 명령을 입력하여 시스템 디스크 파티션을 봅니다.

   디스크 크기가 증가했는지 확인하려면 `/dev/root`, `/dev/sda5`, `/dev/sda6`, `/dev/sda8` 파티션을 확인해야 합니다.

```
admin> show system disk-space
```

```
admin@Panorama-Ynaveh> show system disk-space

Filesystem      Size  Used Avail Use% Mounted on
/dev/root        16G  3.4G   12G  23% /
none            4.0G   60K  4.0G   1% /dev
/dev/sda5        76G  1.8G   71G   3% /opt/pancfg
/dev/sda6        23G  5.0G   17G  24% /opt/panrepo
tmpfs           4.0G  110M  3.8G   3% /dev/shm
cgroup_root     4.0G     0  4.0G   0% /cgroup
/dev/sda8        92G   52G   35G  60% /opt/panlogs
/dev/loop0       50G  7.4G   40G  16% /opt/mongobuffer
tmpfs            12M     0   12M   0% /opt/pancfg/mgmt/ssl/private
```

Panorama 가상 어플라이언스 설정 완료

Panorama 가상 어플라이언스의 초기 구성 수행을(를) 수행한 후 추가 구성을 위해 다음 작업을 계속합니다.

- Panorama 지원 라이선스 활성화
- Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색
- Panorama용 콘텐츠 및 소프트웨어 업데이트 설치
- Panorama 관리 인터페이스 액세스 및 탐색
- Panorama에 대한 관리 액세스 설정
- 방화벽 관리

Panorama 가상 어플라이언스 변환

평가판 Panorama™ 가상 어플라이언스를 Production Panorama 가상 어플라이언스로 변환하여 기존 구성을 유지하고 관리 플랫폼 활용을 시작할 수 있습니다.

ELA(Enterprise License Agreement) 라이선스를 사용하는 경우 기존 Production Panorama 가상 어플라이언스를 변환하여 ELA 라이선스의 이점을 활용할 수 있습니다.

- 로컬 로그 수집기를 사용하여 평가판 Panorama를 Production Panorama로 변환
- 평가판 Panorama를 로컬 로그 수집기가 없는 Production Panorama로 변환
- 로컬 로그 수집기를 사용하여 평가판 Panorama를 VM Flex 라이선스로 변환
- 로컬 로그 수집기 없이 평가 Panorama를 VM-Flex 라이선스로 변환
- Production Panorama를 ELA Panorama로 변환

©2024 Palo Alto Networks, Inc.

로컬 로그 수집기를 사용하여 평가판 Panorama를 Production Panorama로 변환

로컬 로그 수집기로 구성된 Panorama 모드의 평가판 Panorama™ 가상 어플라이언스가 있는 경우 평가판 Panorama에서 Production Panorama로 구성을 마이그레이션하고 필요에 따라 수정하여 Production Panorama로 변환할 수 있습니다.

Panorama 가상 어플라이언스의 로그 수집기가 수집한 로그는 마이그레이션할 수 없습니다.

평가판 *Panorama* 가상 어플라이언스에 저장된 로그에 대한 액세스를 유지해야 하는 경우 평가판 Panorama 구성을 Production Panorama로 마이그레이션한 후 평가판 라이선스의 남은 기간 동안 로컬에서 로그에 액세스할 수 있도록 평가판 *Panorama*의 전원을 켜두십시오. 평가판 *Panorama*를 *Production Panorama*에 관리형 수집기로 추가하는 것은 지원되지 않습니다.

STEP 1 | 마이그레이션을 계획합니다.

- 평가판 Panorama 가상 어플라이언스를 Production Panorama 가상 어플라이언스로 변환하기 전에 Panorama 가상 어플라이언스의 소프트웨어를 업그레이드하십시오. 하이퍼바이저에 필요한 최소 PAN-OS 버전에 대한 호환성 매트릭스를 검토하십시오. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- 마이그레이션에 대한 유지 관리 기간을 예약합니다.

STEP 2 | 프로덕션 Panorama 가상 어플라이언스를 설정합니다.

1. Panorama 가상 어플라이언스 설정.
2. Palo Alto Networks CSP(고객 지원 포털)에 Panorama 가상 어플라이언스를 등록합니다.

   Panorama 일련번호와 인증 코드는 Palo Alto Networks의 주문 요약 이메일에서 찾을 수 있습니다.
3. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 3 | Production Panorama 가상 어플라이언스에 대해 Palo Alto Networks CSP(Custer Support Portal)에서 디바이스 관리 라이선스를 활성화합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. 자산 > 디바이스를 선택한 다음 Panorama 가상 어플라이언스를 찾습니다.
3. 작업 열에서 연필 아이콘을 클릭하여 디바이스 라이선스를 편집합니다.
4. 인증 코드 활성화를 선택한 다음 인증 코드를 입력합니다.
5. 동의 및 제출을 선택하여 디바이스 관리 라이선스를 활성화합니다.

STEP 4 | 평가판 Panorama 가상 어플라이언스에서 Panorama 구성을 내보냅니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 `running-config.xml`을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.
4. 내보낸 `running-config.xml` 파일을 찾아 XML 파일의 이름을 바꿉니다. Panorama는 이름이 `running-config.xml`인 XML 파일 가져오기를 지원하지 않으므로 구성을 가져오는 데 필요합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 평가판 Panorama 가상 어플라이언스에서 Production Panorama 가상 어플라이언스로 내보낸 Panorama 구성 스냅샷을 로드합니다.

1. Production Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 Panorama 가상 어플라이언스에서 내보낸 Panorama 구성 파일을 찾은 다음 확인을 클릭합니다.
4. 이름이 지정된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키를 공백(비어 있음)으로 두고 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다.
5. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

STEP 6 | Production Panorama 가상 어플라이언스에서 구성을 수정합니다.

1. **Panorama** > 설정 > 관리를 선택합니다.
2. 일반 설정을 편집하고 호스트 이름을 수정한 다음 확인을 클릭합니다.
3. 관리 인터페이스 설정을 편집하여 관리 IP 주소를 구성하고 확인을 클릭합니다.

   가장 효율적인 접근 방식은 평가판 *Panorama* 가상 어플라이언스에 새 *IP* 주소를 할당하고 *Production Panorama* 가상 어플라이언스에 대해 이전 *IP* 주소를 재사용하는 것입니다. 이렇게 하면 각 방화벽에서 *Panorama IP* 주소를 재구성하지 않고도 평가판 *Panorama* 가상 어플라이언스에 계속 액세스할 수 있고 방화벽이 *Production Panorama* 가상 어플라이언스를 가리킬 수 있습니다.
4. 평가판 Panorama에서 불러온 로그 수집기 구성을 제거합니다.
   1. **Panorama** > **Collector Group**을 선택한 다음 구성된 모든 수집기 그룹을 삭제합니다.
   2. **Panorama** > 관리형 수집기를 선택한 다음 구성된 모든 로그 수집기를 삭제합니다.
5. 커밋 > **Panorama**에 커밋를 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 7 | 로그 컬렉터 및 컬렉터 그룹을 구성합니다.

이전 단계에서 삭제한 관리형 수집기, 수집기 그룹 구성 및 로그 포워딩 구성을 추가하고 로컬 로그 수집기를 추가해야 합니다.

1. 관리형 수집기 구성.
2. 수집기 그룹 구성.
3. Panorama에 대한 로그 포워딩 구성.

STEP 8 | 지원 및 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.

1. **Panorama** > 라이선스를 선택한 다음 라이선스 서버에서 라이선스 키 검색을 선택합니다.
2. 디바이스 관리 라이선스에 올바른 디바이스 수가 표시되는지 확인합니다.
3. **Panorama** > 지원을 선택한 다음 올바른 지원 수준 및 만료 날짜가 표시되는지 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 9 | Production Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. Production Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

평가판 Panorama를 로컬 로그 수집기가 없는 Production Panorama로 변환

Production Panorama 가상 어플라이언스로 변환하도록 구성된 로컬 Log Collector가 없는 Panorama 모드 또는 관리 전용 모드에서 평가판 Panorama 가상 어플라이언스의 일련번호를 변경하십시오.

로컬 로그 수집기가 구성된 경우 로컬 로그 수집기를 사용하여 평가판 Panorama를 Production Panorama로 변환을(를) 참조하십시오.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.

STEP 3 | Palo Alto Networks에서 제공한 일련번호를 입력합니다.

Panorama 일련번호 및 인증 코드는 이전 단계에서 생성한 배포 프로파일에서 가져옵니다.

STEP 4 | 확인을 클릭합니다.

STEP 5 | 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 6 | Panorama 가상 어플라이언스에서 관리 서버를 다시 시작합니다.

1. Panorama CLI에 로그인.
2. 관리 서버를 다시 시작하십시오.

```
admin> ### ##### ### #### ##-##
```

관리 서버를 다시 시작하면 모든 관리자가 *Panorama* 웹 인터페이스 및 *CLI*에서 로그아웃됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 지원 및 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 라이선스를 선택한 다음 라이선스 서버에서 라이선스 키 검색을 선택합니다.
3. 디바이스 관리 라이선스에 올바른 디바이스 수가 표시되는지 확인합니다.
4. **Panorama** > 지원을 선택한 다음 올바른 지원 수준 및 만료 날짜가 표시되는지 확인합니다.

STEP 8 | Production Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. Production Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

로컬 로그 수집기를 사용하여 평가판 Panorama를 VM Flex 라이선스로 변환

로컬 로그 수집기로 구성된 Panorama 모드의 평가판 Panorama™ 가상 어플라이언스가 있는 경우 평가판 Panorama에서 프로덕션 Panorama로 구성을 마이그레이션하고 필요에 따라 수정하여 VM Flex 라이선스가 있는 프로덕션 Panorama로 변환할 수 있습니다.

로컬 로그 수집기가 구성되지 않은 경우 로컬 로그 수집기 없이 평가 Panorama를 VM-Flex 라이선스로 변환을(를) 참조하십시오.

Panorama 가상 어플라이언스의 로그 수집기가 수집한 로그는 마이그레이션할 수 없습니다.

평가판 *Panorama* 가상 어플라이언스에 저장된 로그에 대한 액세스를 유지해야 하는 경우 평가판 Panorama 구성을 Production Panorama로 마이그레이션한 후 평가판 라이선스의 남은 기간 동안 로컬에서 로그에 액세스할 수 있도록 평가판 *Panorama*의 전원을 켜두십시오. 평가판 *Panorama*를 *Production Panorama*에 관리형 수집기로 추가하는 것은 지원되지 않습니다.

STEP 1 | 마이그레이션을 계획합니다.

- ☐ 평가판 Panorama 가상 어플라이언스를 Production Panorama 가상 어플라이언스로 변환하기 전에 Panorama 가상 어플라이언스의 소프트웨어를 업그레이드하십시오. 하이퍼바이저에 필요한 최소 PAN-OS 버전에 대한 호환성 매트릭스를 검토하십시오. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

- ☐ 마이그레이션에 대한 유지 관리 기간을 예약합니다.

STEP 2 | 유연한 VM 시리즈 라이선스 배포 프로파일에서 Panorama 일련번호와 인증 코드를 가져옵니다.

1. Palo Alto Networks 고객 지원 포털(CSP)에 로그인합니다.
2. Panorama 가상 어플라이언스를 활성화하는 배포 프로파일을 생성합니다.
3. Panorama를 프로비저닝하여 Panorama의 일련 번호를 생성합니다.
4. 일련 번호 및 인증 코드를 복사합니다.

STEP 3 | 프로덕션 Panorama 가상 어플라이언스를 설정합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. Panorama 가상 어플라이언스 설정.
3. Palo Alto Networks CSP(고객 지원 포털)에 Panorama 가상 어플라이언스를 등록합니다.

   이전 단계에서 생성한 Panorama 일련 번호 및 인증 코드.
4. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 4 | Production Panorama 가상 어플라이언스에 대해 Palo Alto Networks CSP에서 디바이스 관리 라이선스를 활성화합니다.

1. 자산 > 디바이스를 선택한 다음 Panorama 가상 어플라이언스를 찾습니다.
2. 작업 열에서 연필 아이콘을 클릭하여 디바이스 라이선스를 편집합니다.
3. 인증 코드 활성화를 선택한 다음 인증 코드를 입력합니다.
4. 동의 및 제출을 선택하여 디바이스 관리 라이선스를 활성화합니다.

STEP 5 | 평가판 Panorama 가상 어플라이언스에서 Panorama 구성을 내보냅니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 `running-config.xml`을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.
4. 내보낸 `running-config.xml` 파일을 찾아 XML 파일의 이름을 바꿉니다. Panorama는 이름이 `running-config.xml`인 XML 파일 가져오기를 지원하지 않으므로 구성을 가져오는 데 필요합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 평가판 Panorama 가상 어플라이언스에서 Production Panorama 가상 어플라이언스로 내보낸 Panorama 구성 스냅샷을 로드합니다.

1. Production Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 Panorama 가상 어플라이언스에서 내보낸 Panorama 구성 파일을 찾은 다음 확인을 클릭합니다.
4. 이름이 지정된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키를 공백(비어 있음)으로 두고 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다.
5. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

STEP 7 | Production Panorama 가상 어플라이언스에서 구성을 수정합니다.

1. **Panorama** > 설정 > 관리를 선택합니다.
2. 일반 설정을 편집하고 호스트 이름을 수정한 다음 확인을 클릭합니다.
3. 관리 인터페이스 설정을 편집하여 관리 IP 주소를 구성하고 확인을 클릭합니다.

   가장 효율적인 접근 방식은 평가판 *Panorama* 가상 어플라이언스에 새 *IP* 주소를 할당하고 *Production Panorama* 가상 어플라이언스에 대해 이전 *IP* 주소를 재사용하는 것입니다. 이렇게 하면 각 방화벽에서 *Panorama IP* 주소를 재구성하지 않고도 평가판 *Panorama* 가상 어플라이언스에 계속 액세스할 수 있고 방화벽이 *Production Panorama* 가상 어플라이언스를 가리킬 수 있습니다.
4. 평가판 Panorama에서 불러온 로그 수집기 구성을 제거합니다.
   1. **Panorama** > **Collector Group**을 선택한 다음 구성된 모든 수집기 그룹을 삭제합니다.
   2. **Panorama** > 관리형 수집기를 선택한 다음 구성된 모든 로그 수집기를 삭제합니다.
5. 커밋 > **Panorama**에 커밋를 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 8 | 로그 수집기 및 수집기 그룹을 재구성합니다.

이전 단계에서 삭제한 관리형 수집기, 수집기 그룹 구성 및 로그 포워딩 구성을 추가하고 로컬 로그 수집기를 추가해야 합니다.

1. 관리형 수집기 구성.
2. 수집기 그룹 구성.
3. Panorama에 대한 로그 포워딩 구성.

STEP 9 | 지원 및 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.

1. **Panorama** > 라이선스를 선택한 다음 라이선스 서버에서 라이선스 키 검색을 선택합니다.
2. 디바이스 관리 라이선스에 올바른 디바이스 수가 표시되는지 확인합니다.
3. **Panorama** > 지원을 선택한 다음 올바른 지원 수준 및 만료 날짜가 표시되는지 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 10 | Production Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. Production Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

로컬 로그 수집기 없이 평가 Panorama를 VM-Flex 라이선스로 변환

Production Panorama 가상 어플라이언스로 변환하도록 구성된 로컬 Log Collector가 없는 Panorama 모드 또는 관리 전용 모드에서 평가판 Panorama 가상 어플라이언스의 일련번호를 변경하십시오.

로컬 로그 수집기가 구성된 경우 로컬 로그 수집기를 사용하여 평가판 Panorama를 VM Flex 라이선스로 변환을(를) 참조하십시오.

STEP 1 | 유연한 VM 시리즈 라이선스 배포 프로파일에서 Panorama 일련번호와 인증 코드를 가져옵니다.

1. Palo Alto Networks 고객 지원 포털(CSP)에 로그인합니다.
2. Panorama 가상 어플라이언스를 활성화하는 배포 프로파일을 생성합니다.
3. Panorama를 프로비저닝하여 Panorama의 일련 번호를 생성합니다.
4. 일련 번호 및 인증 코드를 복사합니다.

STEP 2 | Panorama 웹 인터페이스에 로그인합니다.

STEP 3 | **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.

STEP 4 | Palo Alto Networks에서 제공한 일련번호를 입력합니다.

이전 단계에서 생성한 Panorama 일련 번호 및 인증 코드.

STEP 5 | 확인을 클릭합니다.

STEP 6 | 커밋 및 **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 가상 어플라이언스에서 관리 서버를 다시 시작합니다.

1. Panorama CLI에 로그인.
2. 관리 서버를 다시 시작하십시오.

```
admin> ### ##### ### #### ##-##
```

관리 서버를 다시 시작하면 모든 관리자가 *Panorama* 웹 인터페이스 및 *CLI*에서 로그아웃됩니다.

STEP 8 | 지원 및 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 라이선스를 선택한 다음 라이선스 서버에서 라이선스 키 검색을 선택합니다.
3. 디바이스 관리 라이선스에 올바른 디바이스 수가 표시되는지 확인합니다.
4. **Panorama** > 지원을 선택한 다음 올바른 지원 수준 및 만료 날짜가 표시되는지 확인합니다.

STEP 9 | Production Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. Production Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

Production Panorama를 ELA Panorama로 변환

Production Panorama™ 가상 어플라이언스를 변환하여 ELA 라이선스의 이점으로 Panorama를 계속 활용할 수 있습니다. 프로덕션 배포를 변환하려면 Panorama에 아웃바운드 인터넷 액세스 권한이 있어야 합니다.

Production Panorama를 ELA 라이선스로 변환하는 것은 로컬 로그 수집기가 구성되거나 구성되지 않은 관리 전용 및 Panorama 모드에서 지원됩니다. Panorama에 로컬 로그 수집기가 구성된 경우 Panorama를 ELA 라이선스로 변환하려면 Palo Alto Networks에 지원 티켓을 제출해야 합니다.

©2024 Palo Alto Networks, Inc.

*Production Panorama*에서 *ELA* 라이선스로 변환하는 동안 로컬 로그 수집기가 구성된 경우 *Panorama* 일련번호를 변경하지 마십시오.

로그 수집기의 일련번호가 변경되면 로컬 로그 수집기의 로그에 액세스할 수 없게 되고 수집기 그룹의 다른 로그 수집기가 액세스할 수 없게 되어 더 이상 로그를 수집하지 않을 수 있습니다.

STEP 1 | Panorama를 ELA 라이선스로 전환하십시오.

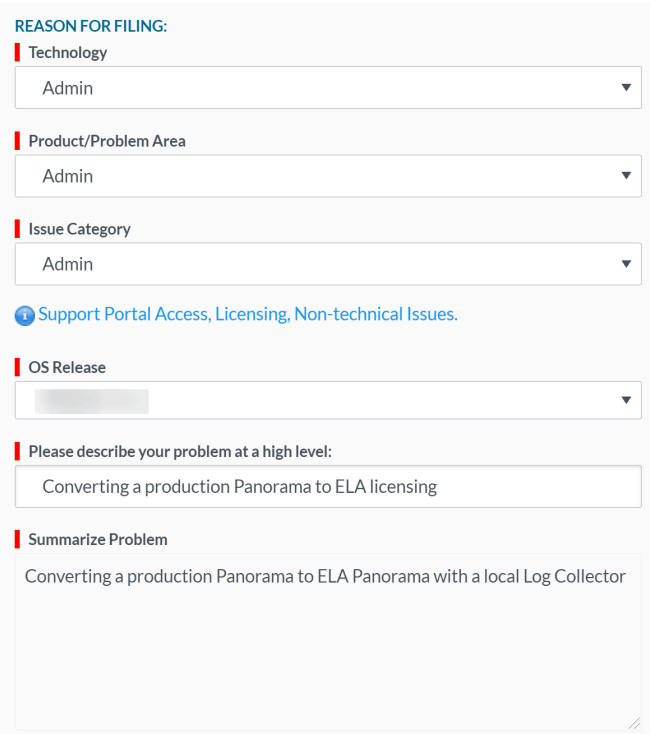
- 로컬 로그 수집기가 있는 **Panorama** 모드의 **Panorama** 가상 어플라이언스.

  Panorama를 ELA 라이선스로 변환하려면 Palo Alto Networks에 지원 티켓을 제출하십시오. 이는 로컬 Log Collector가 있는 Panorama를 ELA 라이선스로 변환할 때 로컬 Log Collector의 모든 기

 ©2024 Palo Alto Networks, Inc.

존 로그를 보존하기 위해 필요합니다. 지원 티켓을 제출하는 데 도움이 되도록 아래에 예가 제공됩니다. 아래 표시된 대로 정확히 티켓을 생성하고 Panorama가 실행 중인 **OS** 릴리스를 선택합니다.

Palo Alto Networks 지원에서 지원 티켓을 성공적으로 해결한 후에만 다음 단계를 계속하십시오.



- 로컬 로그 수집기가 없는 관리 전용 모드 또는 **Panorama** 모드의 **Panorama** 가상 어플라이언스.
  1. ELA 라이선스 풀에서 일련번호를 생성합니다.
     1. Palo Alto Networks CSP에 로그인합니다.
     2. **Assets** > **VM-Series Auth-Codes**를 선택한 다음 ELA 라이선스 풀을 찾습니다.
     3. 작업 열에서 **Panorama**를 선택한 다음 새 일련번호를 프로비저닝합니다.

        메시지가 표시되면 새 일련번호 제공을 확인합니다.
     4. 새로 프로비저닝된 일련번호를 복사합니다.
  2. Panorama 웹 인터페이스에 로그인합니다.
  3. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
  4. 프로비저닝한 일련번호를 입력합니다.
  5. 확인을 클릭합니다.
  6. 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 2 | 아직 로그인하지 않은 경우 Panorama 웹 인터페이스에 로그인합니다.

STEP 3 | **Panorama** > 라이선스를 선택한 다음 라이선스 서버에서 새 라이선스 검색을 선택합니다.

STEP 4 | Panorama가 ELA 계약에 따라 새 라이선스를 검색했는지 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 지원 및 디바이스 관리 라이선스가 성공적으로 활성화되었는지 확인합니다.

1. **Panorama** > 라이선스를 선택한 다음 올바른 라이선스가 활성화되었는지 확인합니다.
2. **Panorama** > 지원을 선택한 다음 올바른 지원 수준 및 만료 날짜가 표시되는지 확인합니다.

©2024 Palo Alto Networks, Inc.

M-시리즈 어플라이언스 설정

M-700, M-600, M-500, M-300 및 M-200 어플라이언스는 관리 전용 모드(로컬 로그 수집이 없는 Panorama 관리 서버), Panorama 모드(로컬 로그 수집이 있는 Panorama 관리 서버) 또는 로그 수집기 모드(전용 로그 수집기로)로 배포할 수 있는 고성능 하드웨어 어플라이언스입니다. 어플라이언스는 방화벽 관리 및 로그 수집과 같은 다양한 Panorama 서비스에 할당할 수 있는 여러 인터페이스를 제공합니다. 어플라이언스를 설정하기 전에 인터페이스를 구성하여 보안을 최적화하고, 네트워크 세분화(대규모 배포에서)를 활성화하고, Panorama 서비스에 대한 트래픽 로드 밸런싱을 수행하는 방법을 고려하십시오.

- M-시리즈 어플라이언스 인터페이스
- M-시리즈 어플라이언스의 초기 구성 수행
- 에어 갭 M-Series 어플라이언스의 초기 구성 수행
- M-시리즈 설정 개요
- M-시리즈 어플라이언스를 로그 수집기로 설정
- M-시리즈 어플라이언스의 스토리지 늘리기
- 다중 인터페이스를 사용하도록 Panorama 구성

M-시리즈 어플라이언스 인터페이스

Panorama M-700, M-600, M-500, M-300, M-200 및 M-100 어플라이언스에는 관리형 방화벽 및 Panorama 관리자의 클라이언트 시스템과 같은 다른 시스템과 통신하기 위한 여러 인터페이스가 있습니다. Panorama는 이러한 시스템과 통신하여 디바이스(방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터) 관리, 로그 수집, 수집기 그룹과 통신, 디바이스에 소프트웨어 및 콘텐츠 업데이트 배포, Panorama에 대한 관리 액세스 제공 등의 다양한 서비스를 수행합니다. 기본적으로 Panorama는 이러한 모든 서비스에 대해 관리(MGT) 인터페이스를 사용합니다. 그러나 관리 액세스를 위해 MGT 인터페이스를 예약하고 다른 서비스에 대해 별도의 전용 인터페이스를 지정하여 보안을 향상시킬 수 있습니다. 여러 하위 네트워크와 많은 로그 트래픽이 있는 대규모 네트워크에서 디바이스 관리 및 로그 수집을 위해 여러 인터페이스를 사용하면 네트워크 분할 및 로드 밸런싱도 가능합니다(다중 인터페이스를 사용하도록 Panorama 구성 참조).

Panorama 서비스를 다양한 인터페이스에 할당할 때 MGT 인터페이스만 구성 및 모니터링 작업을 위해 Panorama에 대한 관리 액세스를 허용한다는 점에 유의하십시오. M-시리즈 어플라이언스의 초기 구성 수행할 때 다른 서비스에 인터페이스를 할당할 수 있습니다. M-시리즈 어플라이언스 하드웨어 참조 가이드에서는 인터페이스용 케이블을 연결하는 위치에 대해 설명합니다. M-100 어플라이언스는 모든 인터페이스에서 1Gbps 처리량을 지원합니다. MGT, Eth1, Eth2 및 Eth3. 이러한 인터페이스 외에도 M-500 어플라이언스는 Eth4 및 Eth5 인터페이스에서 10Gbps 처리량을 지원합니다.

*M-700*을 제외한 *M* 시리즈 어플라이언스는 통합 인터페이스를 위한 *LACP(Link Aggregation Control Protocol)*를 지원하지 않습니다. *M-700*은 집계 인터페이스 *bond1*에 대해 *LACP*를 지원합니다.

©2024 Palo Alto Networks, Inc.

지원되는 인터페이스

인터페이스는 디바이스 관리, 로그 수집, 수집기 그룹 통신, 라이선스 및 소프트웨어 업데이트에 사용할 수 있습니다. 네트워크 분할에 대한 자세한 내용은 다중 인터페이스를 사용하도록 Panorama 구성을(를) 참조하십시오.

상호 작용	최대 속도	M-700 어플라이언스	M-600 어플라이언스	M-500 어플라이언스	M-300 어플라이언스	M-200 어플라이언스
관리(MGT)	1Gbps	✓	✓	✓	✓	✓
이더넷 1(Eth1)	1Gbps	✓	✓	✓	✓	✓
이더넷 2(Eth2)	1Gbps	—	✓	✓	—	✓
이더넷 3(Eth3)	1Gbps	—	✓	✓	—	✓
이더넷 4(Eth4)	10Gbps	—	✓	✓	—	—
이더넷 5(Eth5)	10Gbps	—	✓	✓	—	—

M-700 어플라이언스에는 후면 패널에 이더넷 *1/2* 및 이더넷 *1/3*이라고 표시된 두 개의 포트가 있습니다. 그러나 어플라이언스는 별도의 *Eth2* 및 *Eth3* 하위 인터페이스 대신 ***bond1***이라는 *10Gb* 통합 소프트웨어 인터페이스를 사용합니다.

로깅 속도

모든 M-시리즈 어플라이언스 모델에 대한 로깅 속도를 검토하십시오. 아래 나열된 로깅 속도를 달성하려면 M-시리즈 어플라이언스가 수집기 그룹의 단일 로그 수집기여야 하며 M-시리즈 모델에 대한 모든 로깅 디스크를 설치해야 합니다. 예를 들어, M-500 어플라이언스에 대해 초당 30,000개의 로그를 달성하려면 1TB 또는 2TB 디스크가 있는 12개의 로깅 디스크를 모두 설치해야 합니다.

모델 용량 및 기능	M-700 어플라이언스	M-600 어플라이언스	M-500 어플라이언스	M-300 어플라이언스	M-200 어플라이언스
관리 전용 모드에서 Panorama에 대한 최대 로깅 속도	로컬 로그 스토리지는 지원되지 않습니다.				

©2024 Palo Alto Networks, Inc.

모델 용량 및 기능	M-700 어플라이언스	M-600 어플라이언스	M-500 어플라이언스	M-300 어플라이언스	M-200 어플라이언스
Panorama 모드에서 Panorama에 대한 최대 로깅 속도	36,500 로그/초	25,000로그/초	20,000로그/초	16,500 로그/초	10,000로그/초
로그 수집기 모드에서 Panorama에 대한 최대 로깅 속도	73,000 로그/초	50,000로그/초	30,000로그/초	33,000 로그/초	28,000로그/초
어플라이언스의 최대 로그 스토리지	48TB(12x8TB RAID 디스크)	48TB(12x8TB RAID 디스크)	• 24TB(24x2TB RAID 디스크) • 12TB(24x1TB RAID 디스크)	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)
어플라이언스의 기본 로그 스토리지	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)	4TB(4x2TB RAID 디스크)	16TB(4x8TB RAID 디스크)	16TB(4x8TB RAID 디스크)
어플라이언스의 SSD 스토리지(M-시리즈 어플라이언스가 생성하는 로그용)	240GB	240GB	240GB	240GB	240GB
NFS 연결 로그 스토리지	사용할 수 없습니다				

M-시리즈 어플라이언스의 초기 구성 수행

기본적으로 Panorama의 IP 주소는 192.168.1.1이고 사용자 이름/암호는 admin/admin입니다. 보안상의 이유로 다른 구성 작업을 계속하기 전에 이러한 설정을 변경해야 합니다. MGT(관리) 인터페이스에서 또는 M-700, M-600, M-500, M-300 또는 M-200 어플라이언스의 콘솔 포트에 대한 직접 직렬 포트 연결을 사용하여 이러한 초기 구성 작업을 수행해야 합니다.

10GB 인터페이스가 있는 *Log Collector* 모드에서 *M*-시리즈 어플라이언스를 구성하는 경우 *10GB* 인터페이스가 *Up*으로 표시되도록 이 전체 구성 절차를 완료해야 합니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 네트워크 관리자로부터 필요한 인터페이스와 서버 정보를 수집하십시오.

- 구성하려는 각 인터페이스(MGT, Eth1, Eth2, Eth3, Eth4, Eth5)에 대한 IP 주소, 넷마스크(IPv4의 경우) 또는 접두사 길이(IPv6의 경우) 및 기본 게이트웨이를 수집합니다. MGT 인터페이스만 필수입니다.

  *Palo Alto Networks*는 *MGT* 인터페이스에 대해 이러한 모든 설정을 지정할 것을 권장합니다. 이러한 설정 중 일부(예: 기본 게이트웨이)에 대한 값을 생략하면 향후 구성 변경을 위해 콘솔 포트를 통해서만 *Panorama*에 액세스할 수 있습니다. 이러한 설정을 모두 지정하지 않으면 다른 인터페이스에 대한 구성을 커밋할 수 없습니다.

  어플라이언스를 Panorama 관리 서버로 사용하려는 경우 Palo Alto Networks는 Panorama 관리에만 MGT 인터페이스를 사용하고 디바이스 관리, 로그 수집, Collector Group과의 통신 및 디바이스 업데이트 배포에 다른 인터페이스를 사용할 것을 권장합니다(M- 시리즈 어플라이언스 인터페이스).

- DNS 서버의 IP 주소를 수집합니다.

STEP 2 | 컴퓨터에서 M-시리즈 어플라이언스에 액세스합니다.

1. 다음 방법 중 하나로 M-시리즈 어플라이언스에 연결합니다.
   - 컴퓨터의 직렬 케이블을 M-시리즈 어플라이언스의 콘솔 포트에 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - 컴퓨터의 RJ-45 이더넷 케이블을 M-시리즈 어플라이언스의 MGT 포트에 연결합니다. 브라우저에서 https://192.168.1.1로 이동합니다. 이 URL에 대한 액세스를 활성화하려면 컴퓨터의 IP 주소를 192.168.1.0 네트워크의 주소(예: 192.168.1.2)로 변경해야 할 수 있습니다.
2. 메시지가 표시되면 기본 사용자 이름과 암호(admin/admin)를 사용하여 웹 인터페이스에 로그인합니다. 어플라이언스가 초기화를 시작합니다.

STEP 3 | 기본 관리자 암호를 변경합니다.

*PAN-OS 9.0.4*부터는 사전 정의된 기본 관리자 암호(관리자/관리자)를 디바이스의 첫 번째 로그인에서 변경해야 합니다. 새 암호는 최소 *8*자여야 하며 최소 한 개의 소문자와 하나의 대문자 문자와 하나의 숫자 또는 특수 문자를 포함해야 합니다.

암호 강도에 대한 모범 사례를 사용하여 엄격한 암호를 확인하고 암호 복잡성 설정을 검토해야 합니다.

1. 웹 인터페이스의 왼쪽 하단에 있는 관리자 링크를 클릭합니다.
2. 이전 암호, 새 암호 및 새 암호 확인을 입력하고 확인을 클릭합니다. 새 암호를 안전한 위치에 저장합니다.

   MGT 인터페이스가 안전하게 유지되도록 하려면 최소 암호 복잡성 설정을 구성하고(***Panorama*** > ***Setup*** > ***Management*** 선택) 관리자가 암호를 변경해야 하는 간격을 지정합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama를 관리하고, 디바이스를 관리하고, 로그를 수집하고, Collector Group과 통신하고, 디바이스에 업데이트를 배포하는 데 사용할 각 인터페이스에 대한 네트워크 액세스 설정을 구성합니다.

IPv6 IP 주소를 사용하여 *Panorama*에 대한 연결을 구성하려면 *IPv6 IP* 주소를 사용하여 *Panorama*를 성공적으로 구성하도록 *IPv4* 및 *IPv6*을 모두 구성해야 합니다. *Panorama*는 *IPv6 IP* 주소만으로 관리 인터페이스를 구성하는 것을 지원하지 않습니다.

1. **Panorama** > **Setup** > **Interfaces**를 선택한 다음 인터페이스 이름을 클릭합니다.
2. (비 MGT 인터페이스만 해당) 인터페이스를 활성화합니다.
3. Panorama에서 사용할 각 인터페이스의 네트워크 액세스 설정을 편집합니다. MGT 인터페이스만 필요합니다. Eth1, Eth2, Eth3, Eth4 및 Eth5 인터페이스는 선택 사항이며 M 시리즈 어플라이언스를 Panorama 관리 서버로 사용하려는 경우에만 적용됩니다.
   1. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.

      IPv4—공용 **IP** 주소, **IP** 주소, 넷마스크 및 기본 게이트웨이

      방화벽이 개인 *IP* 주소*(NAT)*로 변환된 공용 *IP* 주소를 사용하여 *Panorama* 관리 서버에 연결하는 경우 공용 ***IP*** 주소 필드에 공용 *IP*를 입력하고 ***IP*** 주소 필드에 개인 *IP*를 입력하여 두 주소를 모두 방화벽에 푸시합니다.

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   2. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 관리 및 디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.

      디바이스 배포(소프트웨어 및 콘텐츠 업데이트) - 하나의 인터페이스만 할당할 수 있습니다.
   3. (선택 사항) 인터페이스가 지원하는 네트워크 연결 서비스를 선택합니다.

      (MGT 인터페이스만 해당) ***Telnet*** 및 ***HTTP***를 비활성화합니다. 이러한 서비스는 일반 텍스트를 사용하므로 다른 서비스보다 덜 안전합니다.
   4. 확인을 클릭하여 변경 사항을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 호스트 이름, 시간대 및 일반 설정을 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
2. Panorama의 시계와 관리형 방화벽을 맞춰 동일한 시간대(예: GMT 또는 UTC)를 사용합니다. Strata Logging Service를 사용하려는 경우, Panorama가 Strata Logging Service와 동기화될 수 있도록 NTP를 구성해야 합니다.

   방화벽은 로그를 생성할 때 타임스탬프를 기록하고 Panorama는 로그를 수신할 때 타임스탬프를 기록합니다. 시간대를 맞추면 타임스탬프가 동기화되고 Panorama에서 로그를 쿼리하고 보고서를 생성하는 프로세스가 조화롭게 이루어집니다.
3. 서버의 호스트 이름을 입력합니다. Panorama는 이를 어플라이언스의 표시 이름/레이블로 사용합니다. 예를 들어, 이것은 CLI 프롬프트에 나타나는 이름입니다. **Panorama** > 관리형 수집기 페이지에서 어플라이언스를 관리형 수집기로 추가하는 경우 수집기 이름 필드에도 나타납니다.
4. (선택 사항) 세계 지도에서 M 시리즈 어플라이언스를 정확하게 배치하려면 위도 및 경도를 입력합니다. 앱 범위 > 트래픽 지도 및 앱 범위 > 위협 지도가 이 값을 사용합니다.
5. 확인을 클릭하여 항목을 저장합니다.

STEP 6 | DNS 서버 및 Palo Alto Networks 업데이트 서버를 구성합니다.

1. **Panorama** > 설정 > 서비스를 선택한 다음 설정을 편집합니다.
2. 기본 **DNS** 서버의 IP 주소와 보조 **DNS** 서버(선택 사항)를 입력합니다.
3. 업데이트 서버의 **URL** 또는 고정 주소(기본값 updates.paloaltonetworks.com)를 입력합니다.

   *Panorama*가 소프트웨어 또는 콘텐츠 패키지를 다운로드하는 업데이트 서버에 신뢰할 수 있는 기관이 서명한 *SSL* 인증서가 있는지 확인하도록 하려면 업데이트 서버 ***ID*** 확인을 선택합니다. 이 옵션은 *Panorama* 관리 서버와 업데이트 서버 간의 통신을 위한 추가 보안 수준을 추가합니다.
4. 확인을 클릭하여 항목을 저장합니다.

STEP 7 | 구성 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

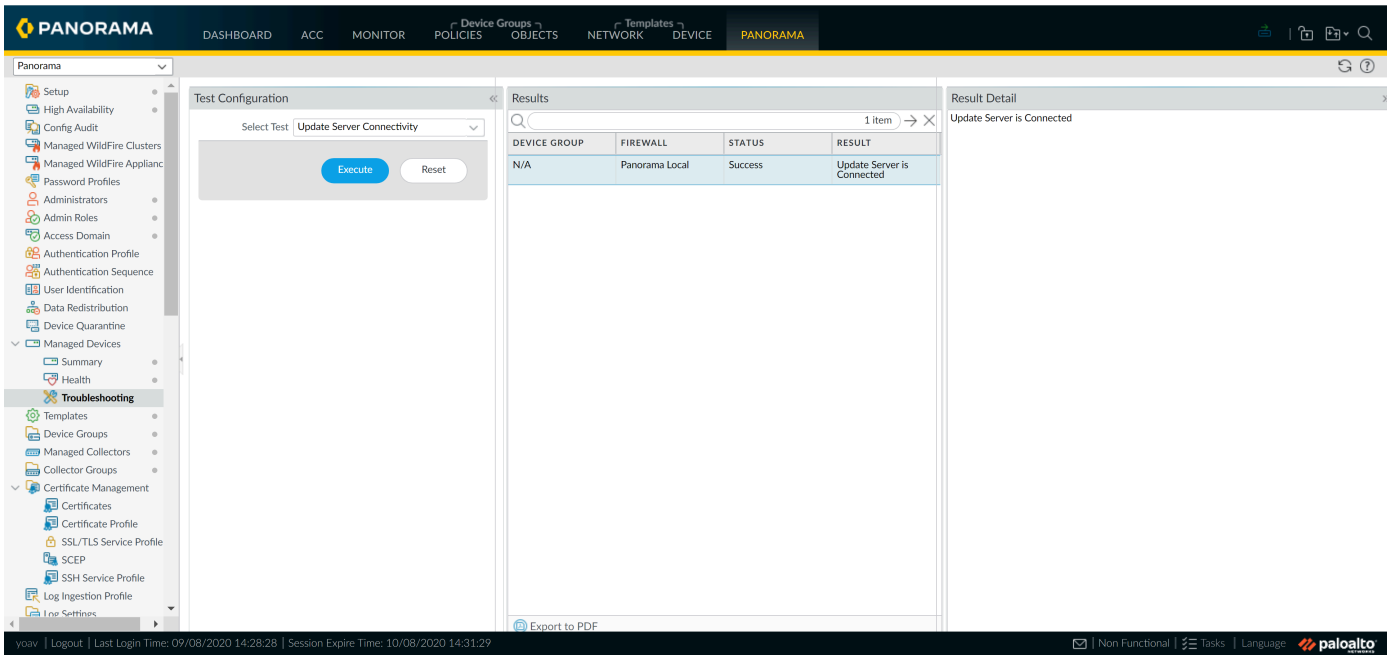


M-Series 어플라이언스를 *Panorama* 관리 서버로 사용할 계획이고 *MGT* 이외의 인터페이스를 구성한 경우 관리형 수집기를 구성할 때 이러한 인터페이스를 ***Device Log Collection*** 또는 ***Collector Group Communication*** 기능에 할당해야 합니다. 인터페이스가 작동하도록 하려면 관리되는 수집기에 대한 수집기 그룹을 구성하고 수집기 그룹 커밋을 수행해야 합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | Palo Alto Networks Update Server와 같은 Panorama 관리에 필요한 외부 서비스에 대한 네트워크 액세스를 확인합니다.

1. 다음 방법 중 하나로 M-시리즈 어플라이언스에 연결합니다.
   - 컴퓨터의 직렬 케이블을 M-시리즈 어플라이언스의 콘솔 포트에 연결합니다. 그런 다음 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 초기 구성 중에 M-시리즈 어플라이언스의 MGT 인터페이스에 대해 지정한 IP 주소에 대한 SSH 세션을 엽니다.
2. 메시지가 표시되면 CLI에 로그인합니다. 초기 구성 중에 지정한 기본 관리자 계정과 암호를 사용합니다.
3. 업데이트 서버 연결 테스트를 사용하여 다음 예와 같이 Palo Alto Networks 업데이트 서버에 대한 네트워크 연결을 확인하십시오.
   1. **Panorama** > **Managed Devices** > **Troubleshooting**을 선택한 다음 테스트 선택 드롭다운에서 서버 연결 업데이트를 선택합니다.
   2. 업데이트 서버 연결 테스트를 실행합니다.



4. 다음 CLI 명령을 사용하여 업데이트 서버에서 Panorama에 대한 지원 자격에 대한 정보를 검색합니다.

```
admin> request support check
```

연결이 있는 경우 업데이트 서버는 Panorama에 대한 지원 상태로 응답합니다. Panorama가 등록되지 않았기 때문에 업데이트 서버는 다음 메시지를 반환합니다.

```
https://www.paloaltonetworks.com/company/contact-us.html
 Support Home https://www.paloaltonetworks.com/support/tabs/
overview# ### ####. # #### #### ##### ## # ####.
```

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 다음 단계...

1. Panorama를 등록하고 라이선스를 설치합니다.
2. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.



가장 좋은 방법은 *Panorama*가 *MGT* 인터페이스를 통해 *HTTPS* 트래픽을 보호하는 데 사용하는 기본 인증서를 교체하는 것입니다.

에어 갭 M-Series 어플라이언스의 초기 구성 수행

에어 갭 M-Series 어플라이언스에 대한 초기 구성을 수행합니다. 기본적으로 Panorama의 IP 주소는 192.168.1.1이고 사용자 이름/암호는 admin/admin입니다. 보안상의 이유로 다른 구성 작업을 계속하기 전에 이러한 설정을 변경해야 합니다. MGT(관리) 인터페이스에서 또는 M-700, M-600, M-500, M-300 또는 M-200 어플라이언스의 콘솔 포트에 대한 직접 직렬 포트 연결을 사용하여 이러한 초기 구성 작업을 수행해야 합니다.

아웃바운드 인터넷 연결이 필요하기 때문에 에어 갭 Panorama를 Palo Alto Networks 업데이트 서버에 연결할 수 없습니다. 라이선스를 활성화하고, PAN-OS 소프트웨어 버전을 업그레이드하고, 동적 콘텐츠 업데이트를 설치하려면 관련 파일을 에어 갭 방화벽에 수동으로 업로드해야 합니다.



10GB 인터페이스가 있는 *Log Collector* 모드에서 *M*-시리즈 어플라이언스를 구성하는 경우 *10GB* 인터페이스가 *Up*으로 표시되도록 이 전체 구성 절차를 완료해야 합니다.

STEP 1 | 네트워크 관리자로부터 필요한 정보를 수집합니다.

- 관리(MGT) 포트의 프라이빗 IP 주소
- 넷마스크(netmask)
- 기본 게이트웨이
- DNS 서버 주소
- NTP 서버 주소

STEP 2 | M-Series 어플라이언스에 설치 및 전원을 공급합니다.

자세한 내용과 모범 사례는 M-Series 어플라이언스 하드웨어 참조 가이드를 확인하십시오.

©2024 Palo Alto Networks, Inc.

STEP 3 | M-Series 어플라이언스에 연결합니다.

기본 ### 사용자 이름을 사용하여 로그인해야 합니다. 계속 진행하기 전에 기본 ### 암호를 변경하라는 메시지가 바로 표시됩니다. 새 암호는 최소 8자여야 하며 최소 한 개의 소문자와 하나의 대문자 문자와 하나의 숫자 또는 특수 문자를 포함해야 합니다.

다음 방법 중 하나로 M-Series 어플라이언스에 연결합니다.

- 컴퓨터의 직렬 케이블을 콘솔 포트에 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 M-시리즈 기기에 연결합니다. 부팅 시퀀스가 완료될 때까지 몇 분 간 기다립니다. M-Series 어플라이언스가 준비되면 M-Series 이름(예: `M-500 ###`)이 변경됩니다.
- 컴퓨터의 RJ-45 이더넷 케이블을 방화벽의 M-Series 어플라이언스에 연결하여 Panorama CLI에 로그인합니다. 브라우저에서 **`https://192.168.1.1`**로 이동합니다.

  이 *URL*에 액세스하려면 컴퓨터의 *IP* 주소를 *192.168.1.0/24* 네트워크의 주소(예: *192.168.1.2*)로 변경해야 할 수 있습니다.

STEP 4 | 에어 갭 M-Series 어플라이언스에 대한 네트워크 설정을 구성합니다.

다음 명령은 인터페이스 IP 할당을 `static`으로 설정하고 MGT 인터페이스, 도메인 이름 서버(DNS) 및 네트워크 시간 프로토콜(NTP) 서버의 IP 주소를 구성합니다.

```
admin> configure
```

```
admin# set deviceconfig system type static
```

```
admin# set deviceconfig system ip-address <IP-Address> netmask
 <Netmask-IP> default-gateway <Gateway-IP>
```

```
admin# set deviceconfig system dns-settings servers primary <IP-
Address> secondary <IP-Address>
```

```
admin# set deviceconfig system ntp-servers primary-ntp-server ntp-
server-address <IP-Address>
```

```
admin# set deviceconfig system ntp-servers secondary-ntp-server
 ntp-server-address <IP-Address>
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Palo Alto Networks 고객 지원 포털(CSP)에 M-Series 어플라이언스를 등록합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. 디바이스 등록을 클릭합니다.
3. 일련번호를 사용하여 디바이스 등록을 선택한 후 다음을 클릭합니다.
4. 필요한 #### ##를 입력합니다.
   - M-Series 어플라이언스의 일련번호를 입력합니다.
   - 디바이스가 오프라인으로 사용됩니다를 선택(활성화)합니다.
   - M-Series 어플라이언스에서 실행 중인 PAN-OS **OS** 릴리즈를 선택합니다.
5. 필요한 ## ##를 입력합니다.
   - M-Series 어플라이언스가 위치한 도시를 입력합니다.
   - M-Series 어플라이언스가 위치한 우편번호를 입력합니다.
   - M-Series 어플라이언스가 위치한 국가를 입력합니다.
6. 동의 및 제출.
7. 선택적 `Day 1` ## 구성 파일을 생성하라는 메시지가 표시되면 이 단계를 건너뛰십시오.

STEP 6 | Panorama 라이선스 키를 다운로드합니다.

라이선스 키 파일은 에어 갭 시 Panorama 라이선스를 활성화할 때 필요합니다.

1. Palo Alto Networks CSP에 로그인합니다.
2. 제품 > 디바이스를 선택하고 추가한 M-Series 어플라이언스를 찾습니다.
3. #### 열의 다운로드 링크에서 모든 라이선스 키 파일을 다운로드합니다.

   Panorama에서 활성화하려는 각 라이선스에 대해 라이선스 키 파일을 다운로드해야 합니다.

STEP 7 | Panorama 라이선스를 활성화합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 라이선스를 선택하고 수동형으로 라이선스 키 업로드를 선택합니다.

   파일 선택을 클릭하여 이전 단계에서 다운로드한 라이선스 키 파일을 선택하고 확인을 클릭합니다.
3. 이 단계를 반복하여 모든 라이선스를 업로드하고 활성화합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | (선택 사항) 필요에 따라 일반 Panorama 설정을 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
2. Panorama에 대한 호스트 이름을 입력하고 네트워크 도메인 이름을 입력합니다. 도메인 이름은 레이블일 뿐입니다. 도메인에 가입하는 데 사용되지 않습니다.
3. 로그인하려는 사용자에게 Panorama 관리 기능에 액세스할 수 있는 권한이 필요함을 알리는 로그인 배너 텍스트를 입력합니다.

   가장 좋은 방법은 환영하는 표현을 사용하지 않는 것입니다. 또한 법률팀에 배너 메시지를 검토하여 무단 액세스가 금지되어 있음을 적절히 경고하는지 확인하도록 요청해야 합니다.
4. 세계 지도에 M-Series를 정확하게 배치할 수 있도록 위도와 경도를 입력합니다.
5. 확인을 클릭합니다.
6. 커밋 및 **Panorama**에 커밋.

©2024 Palo Alto Networks, Inc.

STEP 9 | Panorama에서 PAN-OS 및 동적 콘텐츠 버전을 업그레이드합니다.

대상 PAN-OS 업그레이드 버전에 대한 자세한 내용은 PAN-OS 업그레이드 가이드 및 PAN-OS 릴리즈 노트를 확인하십시오.

1. Palo Alto Networks CSP에 로그인합니다.
2. 동적 콘텐츠 업데이트를 다운로드합니다.

   Secure Copy Protocol(SCP) 서버를 사용하여 *Panorama*, 관리형 방화벽, 로그 수집기 및 *WildFire* 어플라이언스에 대한 동적 콘텐츠 업데이트를 자동으로 다운로드할 수도 있습니다. *SCP* 서버가 *Palo Alto Networks* 업데이트 서버에서 동적 콘텐츠 업데이트를 다운로드하려면 아웃바운드 인터넷 연결이 필요합니다.

   1. 업데이트 > 동적 업데이트를 선택합니다.
   2. 설치하려는 동적 ### ##을 선택합니다.
   3. 동적 콘텐츠 업데이트를 로컬 디바이스에 다운로드합니다.
   4. 이 단계를 반복하여 필요한 모든 동적 콘텐츠 업데이트를 다운로드합니다.
3. PAN-OS 소프트웨어 업데이트를 다운로드합니다.
   1. 업데이트 > 소프트웨어 업데이트를 선택합니다.
   2. ### ##에서 **Panorama M** 베이스를 선택합니다. ### ##의 경우 모두(기본값) 또는 선호를 선택합니다.
   3. #### 열에서 PAN-OS 버전을 클릭하여 로컬 디바이스에 소프트웨어 이미지를 다운로드합니다.
4. Panorama 웹 인터페이스에 로그인합니다.
5. **Panorama** > 동적 업데이트를 선택하고 다운로드한 동적 콘텐츠 업데이트를 업로드합니다.

   이 단계를 반복하여 모든 동적 콘텐츠 릴리즈 버전을 찾아보고 선택합니다.
6. 동적 콘텐츠 업데이트를 설치합니다.
7. **Panorama** > 소프트웨어를 선택하고 다운로드한 PAN-OS 소프트웨어 이미지를 업로드합니다.
8. PAN-OS 소프트웨어 버전을 설치합니다.

   PAN-OS 소프트웨어 업그레이드 설치를 완료하려면 Panorama를 다시 시작해야 합니다.

STEP 10 | Panorama를 네트워크에 연결합니다.

1. 컴퓨터에서 Panorama를 연결 해제합니다.
2. RJ-45 이더넷 케이블을 사용하여 MGT 포트를 관리 네트워크의 스위치 포트에 연결합니다. Panorama에 케이블을 연결한 스위치 포트가 자동으로 협상할 수 있도록 구성되어 있는지 확인합니다.

M-시리즈 설정 개요

M-시리즈 어플라이언스를 설정하려면 다음 절차를 따르십시오.

- 관리 전용 모드에서 M-시리즈 어플라이언스 설정
- Panorama 모드에서 M-시리즈 어플라이언스 설정

©2024 Palo Alto Networks, Inc.

- 로그 수집기 모드에서 M-시리즈 어플라이언스 설정

관리 전용 모드에서 M-시리즈 어플라이언스 설정

Panorama를 방화벽 및 전용 로그 수집기 관리 전용으로 설정하려면 관리 전용 모드에서 Panorama 관리 서버를 설정하십시오. 관리 전용 모드의 Panorama에는 구성 및 시스템 로그를 제외한 로그 수집 기능이 없으며 로그를 저장하려면 전용 로그 수집기가 필요합니다.

로컬 로그 수집기를 구성한 경우 로그 수집 기능이 없음에도 불구하고 관리 전용 모드로 변경할 때 로컬 로그 수집기가 *Panorama*에 여전히 존재합니다. 로컬 로그 수집기(***Panorama*** > 관리형 수집기)를 삭제하면 로컬 로그 수집기가 기본적으로 사용하는 ***Eth1/1*** 인터페이스 구성이 삭제됩니다. 로컬 로그 수집기를 삭제하려면 Eth1/1 인터페이스를 재구성해야 합니다.

STEP 1 | M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 안내서를 참조하십시오.

STEP 2 | M 시리즈 어플라이언스의 초기 구성 수행.

STEP 3 | Panorama를 등록하고 라이선스를 설치합니다.

STEP 4 | Panorama에 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 5 | 관리 전용 모드로 변경합니다.

1. Panorama CLI에 로그인합니다.
2. Panorama 모드에서 관리 전용 모드로 전환:

   ```
   ## ### ### ## ## ##
   ```
3. **Y**를 입력하여 모드 변경을 확인합니다. Panorama 관리 서버가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 Panorama 관리 서버에 다시 연결하여 Panorama 로그인 프롬프트를 확인합니다.

   CMS ### 프롬프트가 표시되면 Panorama 관리 서버의 재부팅이 완료되지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 Enter 키를 누릅니다.
4. CLI에 다시 로그인합니다.
5. 관리 전용 모드로의 전환이 성공했는지 확인합니다.

   ```
   ### ## ## | ### ## ##
   ```

   모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

   ```
   ### ##:## ##
   ```

STEP 6 | Panorama에 대한 관리 액세스 설정

STEP 7 | 방화벽 관리

STEP 8 | 로그 수집 관리

Panorama 모드에서 M-시리즈 어플라이언스 설정

 ©2024 Palo Alto Networks, Inc.

STEP 1 | M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 안내서를 참조하십시오.

STEP 2 | M 시리즈 어플라이언스의 초기 구성 수행.

STEP 3 | Panorama를 등록하고 라이선스를 설치합니다.

STEP 4 | Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.

STEP 5 | 각 배열을 구성합니다. 이 작업은 RAID 디스크를 로깅에 사용할 수 있도록 하는 데 필요합니다. 선택적으로 디스크를 추가하여 M 시리즈 어플라이언스에서 스토리지를 늘릴 수 있습니다.

STEP 6 | Panorama에 대한 관리 액세스 설정.

STEP 7 | 방화벽을 관리합니다.

STEP 8 | 로그 수집을 관리합니다.

로그 수집기 모드에서 M-시리즈 어플라이언스 설정

STEP 1 | M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 안내서를 참조하십시오.

STEP 2 | M-시리즈 어플라이언스의 초기 구성 수행

STEP 3 | Panorama 등록 및 라이선스 설치

STEP 4 | Panorama용 콘텐츠 및 소프트웨어 업데이트 설치

STEP 5 | 각 배열을 구성합니다. 이 작업은 RAID 디스크를 로깅에 사용할 수 있도록 하는 데 필요합니다. 선택적으로 디스크를 추가하여 M 시리즈 어플라이언스에서 스토리지를 늘릴 수 있습니다.

STEP 6 | M-시리즈 어플라이언스를 로그 수집기로 설정

STEP 7 | 로그 수집 관리

M-시리즈 어플라이언스를 로그 수집기로 설정

로그 수집을 위한 전용 어플라이언스를 원하는 경우 로그 수집기 모드에서 M-200, M-300, M-500, M-600 또는 M-700 어플라이언스를 구성합니다. 이렇게 하려면 먼저 라이선스, 소프트웨어 및 콘텐츠 업데이트 설치, 관리(MGT) 인터페이스 구성을 포함하는 Panorama 모드에서 어플라이언스의 초기 구성을 수행합니다. 그런 다음 M-시리즈 어플라이언스를 로그 수집기 모드로 전환하고 로그 수집기 구성을 완료합니다. 또한 로그 수집 및 수집기 그룹 통신을 위해 MGT 인터페이스 대신 전용 M-시리즈 어플라이언스 인터페이스(권장)를 사용하려면 먼저 Panorama 관리 서버에 대한 인터페이스를 구성한 다음 로그 수집기에 대해 구성해야 합니다. 그런 다음 Panorama 커밋을 수행한 다음 Collector Group 커밋을 수행합니다.

새 M-시리즈 어플라이언스를 로그 수집기로 설정하거나 이전에 Panorama 관리 서버로 배포된 기존 M-시리즈 어플라이언스를 변환하려면 다음 단계를 수행하십시오.

 ©2024 Palo Alto Networks, Inc.

10GB 인터페이스가 있는 *Log Collector* 모드에서 *M*-시리즈 어플라이언스를 구성하는 경우 *10GB* 인터페이스가 *Up*으로 표시되도록 이 전체 구성 절차를 완료해야 합니다.

M-시리즈 어플라이언스를 *Panorama* 모드에서 *Log Collector* 모드로 전환하면 어플라이언스가 재부팅되고, 로컬 *Log Collector*가 삭제되고, 기존 로그 데이터가 삭제되고, 관리 액세스 설정을 제외한 모든 구성이 삭제됩니다. 모드를 전환해도 라이선스, 소프트웨어 업데이트 또는 콘텐츠 업데이트는 삭제되지 않습니다.

STEP 1 | 아직 설정하지 않은 경우 Log Collector를 관리할 Panorama 관리 서버를 설정합니다.

다음 작업 중 하나를 수행합니다.

- Panorama 가상 어플라이언스 설정
- M-시리즈 어플라이언스 설정

STEP 2 | Panorama 관리 서버의 관리 IP 주소를 기록합니다.

고가용성(HA) 구성에서 Panorama를 배포한 경우 각 HA 피어의 IP 주소가 필요합니다.

1. Panorama 관리 서버의 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 확인하여 단독(비 HA) 또는 활성(HA) Panorama의 **IP** 주소를 기록합니다.
3. HA 배포의 경우 **Panorama** > 고가용성을 선택한 다음 설정 섹션을 선택하여 수동 Panorama의 피어 **HA IP** 주소를 기록합니다.

STEP 3 | 전용 로그 수집기 역할을 할 M-시리즈 어플라이언스를 설정합니다.

이전에 이 어플라이언스를 Panorama 관리 서버로 배포한 경우 MGT 인터페이스가 이미 구성되어 있고 라이선스와 업데이트가 이미 설치되어 있으므로 이 단계를 건너뛸 수 있습니다.

Log Collector 모드의 M-Series 어플라이언스에는 구성 작업을 위한 웹 인터페이스가 없고 CLI만 있습니다. 따라서 M-시리즈 어플라이언스에서 모드를 변경하기 전에 Panorama 모드에서 웹 인터페이스를 사용하여 다음을 수행하십시오.

1. M 시리즈 어플라이언스의 초기 구성 수행.
2. Panorama를 등록하고 라이선스를 설치합니다.
3. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.

STEP 4 | M-시리즈 어플라이언스의 CLI에 액세스합니다.

1. 다음 방법 중 하나로 M-시리즈 어플라이언스에 연결합니다.
   - 컴퓨터의 직렬 케이블을 M-시리즈 어플라이언스의 콘솔 포트에 연결합니다. 그런 다음 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 초기 구성 중에 M-시리즈 어플라이언스의 MGT 인터페이스에 대해 지정한 IP 주소에 대한 SSH 세션을 엽니다.
2. 메시지가 표시되면 CLI에 로그인합니다. 초기 구성 중에 지정한 기본 관리자 계정과 암호를 사용합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama 모드에서 로그 수집기 모드로 전환합니다.

1. 다음 명령을 입력하여 로그 수집기 모드로 전환합니다.

```
> request system system-mode logger
```

2. **Y**를 입력하여 모드 변경을 확인합니다. M-시리즈 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 M-시리즈 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 확인하십시오.

   CMS ### 프롬프트가 표시되면 로그 수집기가 재부팅을 완료하지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 *Enter* 키를 누릅니다.

3. CLI에 다시 로그인합니다.
4. 로그 수집기 모드로의 전환이 성공했는지 확인합니다.

```
> show system info | match system-mode
```

   모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

```
system-mode: logger
```

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 로깅 디스크를 RAID1 쌍으로 구성합니다.

이전에 어플라이언스를 Panorama 관리 서버로 배포한 경우 디스크 쌍이 이미 구성되어 사용 가능하므로 이 단계를 건너뛸 수 있습니다.

드라이브를 구성하는 데 필요한 시간은 드라이브의 데이터 양에 따라 몇 분에서 몇 시간까지 다양합니다.

1. M-시리즈 어플라이언스에서 RAID 쌍으로 구성하기 위해 어떤 디스크 쌍이 있는지 확인합니다.

   ```
   > show system raid detail
   ```

   나머지 단계를 수행하여 ## 디스크가 있는 각 디스크 쌍을 구성합니다. 이 예에서는 디스크 쌍 A1/A2를 사용합니다.
2. 쌍의 첫 번째 디스크를 추가하려면 다음 명령을 입력하고 요청을 확인하라는 메시지가 표시되면 **y**를 입력합니다.

   ```
   > request system raid add A1
   ```

   쌍에 다음 디스크를 추가하기 전에 프로세스가 완료될 때까지 기다리십시오. RAID 구성의 진행 상황을 모니터링하려면 다음을 다시 입력하십시오.

   ```
   > show system raid detail
   ```

   첫 번째 디스크에 대한 프로세스가 완료된 후 출력에 디스크 쌍 상태가 ## ##하지만 ### ###으로 표시됩니다.
3. 쌍에 두 번째 디스크를 추가합니다.

   ```
   > request system raid add A2
   ```
4. 디스크 설정이 완료되었는지 확인합니다.

   ```
   > show system raid detail
   ```

   두 번째 디스크에 대한 프로세스가 완료된 후 출력은 디스크 쌍 상태를 ## ## 및 ##로 표시합니다.

   ```
   ### # A       ## ### ##          ##
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Log Collector와 Panorama 관리 서버 간의 연결을 활성화합니다.

로그 수집기 CLI에서 다음 명령을 입력합니다. 여기서 *<IPaddress1>*은(는) 단독(비HA) 또는 활성(HA) Panorama의 MGT 인터페이스용이고 *<IPaddress2>*은(는) 패시브(HA) Panorama의 MGT 인터페이스용입니다.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 8 | 로그 수집기의 일련번호를 기록합니다.

Panorama 관리 서버에서 Log Collector를 관리형 수집기로 추가하려면 일련번호가 필요합니다.

1. Log Collector CLI에서 다음 명령을 입력하여 일련번호를 표시합니다.

   ```
   > show system info | match serial
   ```

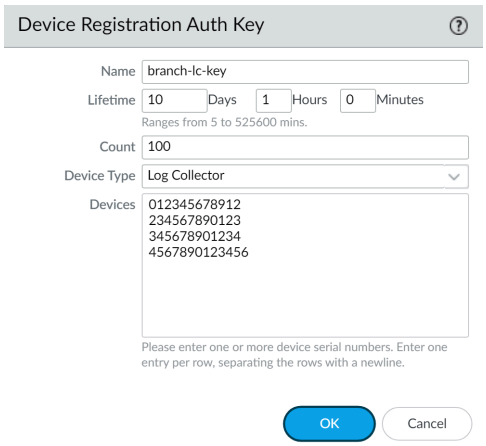
2. 일련번호를 기록하십시오.

 ©2024 Palo Alto Networks, Inc.

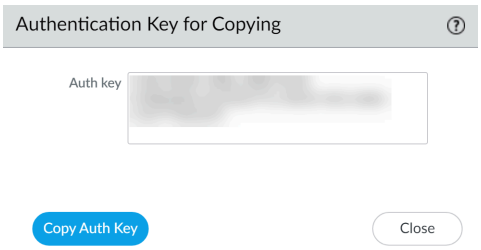
STEP 9 | 기기 등록 인증 키를 생성합니다.

1. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
2. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 기간에 대한 키 수명을 지정합니다.
   - 개수 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 로그 수집기를 인증하는 데만 사용되도록 지정합니다.

     모두를 선택하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩하는 디바이스 등록 인증 키를 사용할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 로그 수집기를 지정할 하나 이상의 디바이스 일련번호를 입력합니다.
3. 확인을 클릭합니다.



4. 인증 키를 복사하고 닫습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 10 | Log Collector를 Panorama 관리 서버에 관리형 수집기로 추가합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 관리형 수집기 추가를 선택합니다.
2. 일반 설정에서 로그 수집기에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
3. **Panorama Server IP** 필드에 단독(비 HA) 또는 활성(HA) Panorama의 IP 주소 또는 FQDN을 입력합니다. HA 배포의 경우 **Panorama Server IP 2** 필드에 패시브 Panorama 피어의 IP 주소 또는 FQDN을 입력합니다.

   이러한 IP 주소는 디바이스 관리 및 디바이스 로그 수집 서비스가 활성화된 Panorama 인터페이스를 지정해야 합니다. 기본적으로 이러한 서비스는 MGT 인터페이스에서만 활성화됩니다. 그러나 Panorama 관리 서버인 M-Series Appliance를 설정할 때 다른 인터페이스에서 서비스를 활성화했을 수 있습니다.
4. 인터페이스를 선택한 다음 관리를 클릭한 후 네트워크의 IP 프로토콜을 기반으로 MGT 인터페이스에 대해 다음 필드 세트 중 하나 또는 둘 다를 구성합니다.
   - IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
5. 확인을 두 번 클릭하여 변경 사항을 로그 수집기에 저장합니다.
6. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

   이 단계는 로깅 디스크를 활성화하기 전에 필요합니다.
7. **Panorama** > 관리형 수집기에 추가한 로그 수집기가 나열되는지 확인합니다. 연결됨 열에는 로그 수집기가 Panorama에 연결되었음을 나타내는 확인 표시가 표시됩니다. 페이지에 업데이트된 연결 상태가 표시될 때까지 몇 분 정도 기다려야 할 수 있습니다.

   이 시점에서 구성 상태 열에는 동기화되지 않음이 표시되고 런타임 상태 열에는 연결 끊김이 표시됩니다. 수집기 그룹을 구성한 후 상태가 동기화 중 및 연결됨으로 변경됩니다(로그 수집기를 수집기 그룹에 할당 단계).

STEP 11 | 로그 수집기에 디바이스 등록 인증 키를 추가합니다.

전용 로그 수집기에만 디바이스 등록 인증 키를 추가합니다. Panorama 모드의 Panorama는 자체 로컬 로그 수집기를 인증할 필요가 없습니다.

1. 로그 수집기 CLI에 로그인합니다.
2. 디바이스 등록 인증 키를 추가합니다.

```
admin> request authkey set <auth-key>
```



STEP 12 | 로깅 디스크를 활성화합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
2. 디스크를 선택한 다음 각 RAID 디스크 쌍을 추가합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 13 | (권장) Panorama 관리 서버 및 로그 수집기가 디바이스 로그 수집(방화벽에서 로그 수신) 및 수집기 그룹 통신에 사용할 경우**Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** 및 **Ethernet5** 인터페이스를 구성합니다.

이전에 Log Collector를 Panorama 관리 서버로 배포하고 이러한 인터페이스를 구성한 경우 Log Collector 모드(Panorama 모드에서 Log Collector 모드로 전환)로 전환하면 관리 액세스 설정을 제외한 모든 구성이 삭제되므로 이를 다시 구성해야 합니다.

1. 아직 구성하지 않은 경우 Panorama 관리 서버에서 각 인터페이스(MGT 인터페이스 제외)를 구성합니다.
   1. **Panorama** > **Setup** > **Interfaces**를 선택한 다음 인터페이스 이름을 클릭합니다.
   2. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
   3. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.

      IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   4. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 관리 및 디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.

      디바이스 배포(소프트웨어 및 콘텐츠 업데이트) - 하나의 인터페이스만 할당할 수 있습니다.
   5. 확인을 클릭하여 변경 사항을 저장합니다.
2. Log Collector의 각 인터페이스(MGT 인터페이스 제외)를 구성합니다.
   1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
   2. 인터페이스를 선택한 다음 인터페이스 이름을 클릭합니다.
   3. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
   4. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.

      IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   5. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.
   6. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
3. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 14 | (선택 사항) 배포에서 Panorama와 관리되는 디바이스 간의 인증에 사용자 지정 인증서를 사용하는 경우 사용자 지정 클라이언트 디바이스 인증서를 배포합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택한 다음 드롭다운에서 인증서 프로파일을 선택하거나 새 인증서 프로파일을 클릭하여 생성합니다.
2. 로그 수집기에 대하여 **Panorama** > 관리형 수집기 > 통신 > 추가를 선택합니다.
3. 보안 클라이언트 통신 체크박스를 선택합니다.
4. 유형 드롭다운에서 디바이스 인증서 유형을 선택합니다.
   - 로컬 디바이스 인증서를 사용하는 경우 해당 드롭다운에서 인증서 및 인증서 프로파일을 선택합니다.
   - SCEP를 디바이스 인증서로 사용하는 경우 해당 드롭다운에서 **SCEP** 프로파일 및 인증서 프로파일을 선택합니다.
5. 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 15 | (선택 사항) 로그 수집기에서 보안 서버 통신을 구성합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 관리형 수집기 > 통신 > 추가를 선택합니다.
2. 사용자 지정 인증서만 확인란이 선택되어 있지 않은지 확인합니다. 이를 통해 사용자 지정 인증서로 마이그레이션하는 동안 모든 디바이스를 계속 관리할 수 있습니다.

   Custom Certificate Only 확인란을 선택하면 *Log Collector*가 인증되지 않고 사전 정의된 인증서를 사용하여 디바이스에서 로그를 수신할 수 없습니다.
3. SSL/TLS 서비스 프로파일 드롭다운에서 **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 로그 수집기와 로그를 보내는 디바이스 간의 모든 SSL 연결에 적용됩니다.
4. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
5. 서버가 관리되는 디바이스의 일련번호에 대해 클라이언트를 확인하도록 하려면 일련번호를 기반으로 클라이언트 인증을 선택합니다. 클라이언트 인증서에는 일련번호를 기반으로 권한을 부여하는 CN으로 특수 키워드 $UDID가 설정되어 있어야 합니다.
6. 연결 끊기 대기 시간(분)에 Panorama가 관리형 디바이스와의 연결을 끊고 다시 설정하기 전에 기다려야 하는 시간(분)을 입력합니다. 이 필드는 기본적으로 비어 있으며 범위는 0~44,640분입니다.

   연결 해제 대기 시간은 새 구성을 커밋할 때까지 카운트다운을 시작하지 않습니다.
7. (선택 사항) 권한 부여 목록을 구성합니다.
   1. 인증 목록에서 추가를 클릭합니다.
   2. 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 선택한 유형의 식별자를 입력합니다.
   4. 확인을 클릭합니다.
   5. 권한 부여 목록 확인을 선택하여 권한 부여 목록을 시행하십시오.
8. 확인을 클릭합니다.
9. 커밋 > **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 16 | 수집기 그룹에 로그 수집기를 할당합니다.

1. 수집기 그룹을 구성합니다. Panorama 커밋을 수행한 다음 수집기 그룹 커밋을 수행하여 로그 수집기 구성을 Panorama와 동기화하고 Eth1, Eth2, Eth3, Eth4 및 Eth5 인터페이스(구성한 경우)를 로그 수집기에서 작동 상태로 전환해야 합니다.

   모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.

   단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화하는 것이 가장 좋습니다. 이 옵션을 사용하려면 각 로그 수집기에 동일한 수의 로깅 디스크가 있어야 합니다.

2. **Panorama** > 관리형 수집기를 선택하여 로그 수집기 구성이 Panorama와 동기화되었는지 확인합니다.

   구성 상태 열은 동기화 중으로 표시되어야 하고 런타임 상태 열은 연결됨으로 표시되어야 합니다.

3. Log Collector CLI에 액세스하고 다음 명령을 입력하여 해당 인터페이스가 작동하는지 확인합니다.

   ```
   > show interface all
   ```

   출력은 ## 중인 각 인터페이스에 대해 작동 ##를 표시합니다.

4. 수집기 그룹에 여러 로그 수집기가 있는 경우 네트워크 리소스에 대한 연결 문제 해결 로그 수집기가 사용하는 각 인터페이스에 대해 Ping 연결 테스트를 수행하여 서로 통신할 수 있는지 확인합니다. ## IP 주소에 대해 로그 수집기 중 하나의 인터페이스를 지정합니다. ### IP 주소에 대해 동일한 수집기 그룹에 있는 다른 로그 수집기와 일치하는 인터페이스를 지정합니다.

STEP 17 | 다음 단계...

Log Collector가 방화벽 로그를 수신하도록 하려면:

1. Panorama에 대한 로그 포워딩을 구성합니다.
2. Panorama로 로그 포워딩 확인.

M 시리즈 어플라이언스의 스토리지 늘리기

M-Series 어플라이언스의 초기 구성을 수행한 후 기존 드라이브 쌍을 더 큰 용량의 드라이브로 업그레이드하거나 빈 드라이브 베이에 추가 드라이브 쌍을 설치하여 어플라이언스의 로그 저장 용량을 늘릴 수 있습니다. 예를 들어 M-500 어플라이언스에서 기존 1TB 드라이브를 2TB로 업그레이드하거나 빈 드라이브 베이(B1 ~ D2)에 2TB 드라이브를 추가할 수 있습니다.

M-시리즈 어플라이언스는 디스크 오류 발생 시 데이터 중복성을 위해 *RAID 1*을 활용합니다. 따라서 *RAID 1* 어레이의 드라이브 쌍은 동일해야 합니다. 그러나 다양한 *RAID 1* 어레이에서 드라이브 용량을 자유롭게 혼합할 수 있습니다. 예를 들어, *A1/A2 RAID 1* 어레이의 드라이브는 *1TB* 드라이브가 될 수 있고 *B1/B2 RAID 1* 어레이의 드라이브는 *2TB* 드라이브가 될 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

다음 표에는 M-시리즈 어플라이언스에서 지원되는 최대 드라이브 베이(디스크) 수와 사용 가능한 드라이브 용량이 나와 있습니다.

각 드라이브 쌍(예: *A1/A2*)이 *RAID 1* 어레이에 있으므로 총 스토리지 용량은 설치된 총 드라이브의 절반입니다. 예를 들어 *M-500* 어플라이언스의 드라이브 베이 *A1/A2* 및 *B1/B2*에 설치된 *2TB* 드라이브가 있는 경우 *A1/A2* 어레이는 총 *2TB*의 스토리지를 제공하고 *B1/B2* 어레이는 총 *4TB*에 대해 다른 *2TB*를 제공합니다.

기구	지원되는 드라이브 베이 수(디스크)	지원되는 드라이브 용량
M-200 기기	4	8TB
M-300 어플라이언스	4	8TB
M-500 기기	24	1TB 또는 2TB
M-600 기기	12	8TB
M-700 어플라이언스	12	8TB

로그 저장 용량을 확장하기 전에 Panorama 로그 저장 요구 사항을 결정하십시오. 단일 M 시리즈 어플라이언스가 지원하는 것보다 더 많은 로그 스토리지가 필요한 경우 전용 로그 수집기를 추가하거나(관리형 수집기 구성 참조) Panorama에서 외부 대상으로의 로그 포워딩을 구성할 수 있습니다.

이미 배포된 *M*-시리즈 어플라이언스에 드라이브를 추가할 때 스토리지를 확장하기 위해 *M*-시리즈 어플라이언스를 오프라인으로 전환할 필요가 없습니다. 추가 드라이브를 구성할 수 있고 사용할 수 있는 경우 *M*-시리즈 어플라이언스는 사용 가능한 모든 드라이브에 로그를 재배포합니다. 이 로그 재배포 프로세스는 백그라운드에서 발생하며 가동 시간이나 *M-Series* 어플라이언스의 가용성에 영향을 미치지 않습니다. 그러나 이 프로세스는 최대 로깅 속도를 줄입니다. 재배포 상태 열(***Panorama*** > ***Collector Groups***)은 프로세스의 완료 상태를 백분율로 나타냅니다.

- M-시리즈 어플라이언스에 추가 드라이브 추가
- M-시리즈 어플라이언스에서 드라이브 업그레이드

M-시리즈 어플라이언스에 추가 드라이브 추가

STEP 1 | 해당 드라이브 베이에 새 드라이브를 설치합니다.

다음에 열려 있는 드라이브 베이에 드라이브를 순차적으로 추가해야 합니다. 예를 들어, C1 및 C2에 드라이브를 추가하기 전에 B1 및 B2에 드라이브를 추가하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | M-시리즈 어플라이언스에서 명령줄 인터페이스(CLI)에 액세스합니다.

다음 두 가지 방법 중 하나로 M-시리즈 어플라이언스에 연결합니다.

- 컴퓨터의 직렬 케이블을 콘솔 포트에 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 M-시리즈 기기에 연결합니다.
- 터미널 에뮬레이션 소프트웨어(예: PuTTY)를 사용하여 M-시리즈 어플라이언스의 IP 주소에 대한 SSH(Secure Shell) 세션을 엽니다.

STEP 3 | 메시지가 표시되면 어플라이언스에 로그인합니다.

기본 관리자 계정과 할당된 암호를 사용합니다.

STEP 4 | 각 어레이를 구성합니다.

드라이브의 데이터를 미러링하는 데 필요한 시간은 드라이브의 데이터 양에 따라 몇 분, 몇 시간 또는 하루 이상이 걸릴 수 있습니다.

다음 예에서는 베이 B1 및 B2의 드라이브를 사용합니다.

1. 다음 명령을 입력하고 메시지가 표시되면 요청을 확인합니다. 이 명령은 M-Series 어플라이언스에 추가하는 디스크의 기존 데이터를 삭제합니다.

```
> ### ### ## ## B1 > ### ### ## ## B2
```

(*RMA만 해당*) 디스크의 데이터를 보존하려면 다음 명령을 대신 사용해 보십시오.

```
> request system raid add B1 force no-format
 > request system raid add B2 force no-format
```

2. RAID 구성의 진행 상황을 모니터링하려면 다음 명령을 입력하십시오.

```
> ### ### ## ## ##
```

RAID 설정이 완료되면 다음 응답이 표시됩니다.

```
### # A       ## ### ##          ### ID A1 ##     ## ##:
 ST91000640NS ###: 953869 MB ##: ### ## ### ID A2     ##       #
#: ST91000640NS ###: 953869 MB ##: ## ### ### # B        ## #
# ##          ### ID B1 ##      ## ##: ST91000640NS ###: 953869
 MB ##: ### ## ### ID B2     ##        ##: ST91000640NS ###:
 953869MB ##: ### ##
```


©2024 Palo Alto Networks, Inc.

STEP 5 | 어레이를 로깅에 사용할 수 있도록 합니다.

로깅을 위해 어레이를 활성화하려면 먼저 기기를 Panorama의 관리형 수집기로 추가해야 합니다. 아직 추가되지 않은 경우 관리형 수집기 구성을 참조하세요.

1. 이 Log Collector를 관리하는 Panorama 관리 서버의 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
3. 디스크를 선택하고 각 어레이를 추가합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.
5. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.
6. 커밋 > 디바이스에 푸시를 선택하고 수집기 그룹을 선택한 다음 변경 사항을 푸시합니다.

M-시리즈 어플라이언스에서 드라이브 업그레이드

STEP 1 | M-시리즈 어플라이언스에서 명령줄 인터페이스(CLI)에 액세스합니다.

다음 두 가지 방법 중 하나로 M-시리즈 어플라이언스에 연결합니다.

- 컴퓨터의 직렬 케이블을 콘솔 포트에 연결하고 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 M-시리즈 기기에 연결합니다.
- 터미널 에뮬레이션 소프트웨어(예: PuTTY)를 사용하여 M-시리즈 어플라이언스의 IP 주소에 대한 SSH(Secure Shell) 세션을 엽니다.

STEP 2 | 메시지가 표시되면 어플라이언스에 로그인합니다.

기본 관리자 계정과 할당된 암호를 사용합니다.

STEP 3 | 설치된 드라이브의 RAID 1 상태가 적어도 2개의 작동하는 RAID 1 어레이가 있음을 나타내는지 확인합니다. 업그레이드하는 동안 RAID 1 어레이를 한 번에 하나씩 업그레이드하며 어플라이언스에서 사용할 수 있는 다른 RAID 1 어레이가 하나 이상 있어야 합니다. 구성에서 작동하는 유일한 어레이를 제거하려고 하면 어플라이언스에 중단 오류가 표시됩니다.

RAID 상태를 보려면 다음 명령을 입력합니다.

```
> show system raid detail
```

예를 들어, 다음은 두 개의 사용 가능한 어레이(디스크 쌍 A 및 디스크 쌍 B)가 있는 M-500 어플라이언스의 출력을 보여줍니다. 사용 가능한 어레이가 하나만 있는 경우 드라이브를 업그레이드하기 전에 M-시리즈 어플라이언스에 추가 드라이브 추가에 설명된 대로 두 번째 어레이를 추가해야 합니다.

```
Disk Pair A                                  Available
 Status                                        clean Disk id
 A1                                Present model        :
 ST91000640NS size          : 953869 MB status       :
 active sync Disk id A2 Present model        : ST91000640NS
 size          : 953869 MB status       : active sync
 Disk Pair B                                 Available
 Status                                        clean Disk id
 B1                                Present model        : ST91000640NS
 size          : 953869 MB status       : active sync Disk id
```

 ©2024 Palo Alto Networks, Inc.

```
B2                              Present model        : ST91000640NS
size          : 953869 MB status       : active sync
```

STEP 4 | 첫 번째 1TB 드라이브를 제거하고 2TB 드라이브로 교체합니다.

1. RAID 1 어레이 구성(이 예에서는 A1)에서 첫 번째 드라이브를 제거하려면 다음 명령을 입력하고 요청을 확인하라는 메시지가 표시되면 **y**를 입력합니다.

   ```
   > request system raid remove A1
   ```

2. 드라이브 베이에서 첫 번째 드라이브를 물리적으로 제거합니다. 드라이브 베이 A1의 드라이브 캐리어에 있는 이젝터 버튼을 눌러 이젝터 핸들을 풉니다. 그런 다음 핸들을 앞으로 당기고 드라이브를 어플라이언스에서 밀어냅니다.
3. 포장에서 2TB 드라이브를 꺼내 방금 제거한 드라이브 옆 테이블에 놓습니다. 동일한 캐리어에 2TB 드라이브를 설치할 것이기 때문에 드라이브가 캐리어에 어떻게 설치되었는지 기록해 두십시오.
4. 캐리어에서 1TB 드라이브를 고정하는 나사 4개를 제거하고 캐리어에서 드라이브를 제거합니다.
5. 1TB 드라이브에서 제거한 것과 동일한 4개의 나사를 사용하여 2TB 드라이브를 캐리어에 부착한 다음 2TB 드라이브가 있는 캐리어를 드라이브 베이 A1에 다시 삽입합니다.
6. 다음 명령을 입력하여 2TB 드라이브가 인식되는지 확인합니다.

   ```
   show system raid detail
   ```

   A1 디스크에 올바른 모델과 크기(약 2TB)가 표시되는지 확인합니다. 모델과 크기가 정확하지 않은 경우 올바른 모델과 크기가 표시될 때까지 위의 명령을 다시 실행합니다.

   잘못된 모델과 크기가 일관되게 표시되면 다음 명령을 입력합니다.

   ```
   request system raid remove A1
   ```

   위 명령어를 실행한 후 30초간 기다린 후 디스크를 제거했다가 다시 삽입하고 **show system raid detail** 명령어를 반복하여 크기와 모델을 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | RAID 1 어레이에 설치된 나머지 1TB 드라이브의 데이터를 해당 어레이에 새로 설치된 2TB 드라이브로 복사합니다.

데이터를 복사하는 데 필요한 시간은 드라이브의 데이터 양에 따라 몇 분에서 몇 시간까지 차이가 날 수 있습니다.

1. 드라이브 베이 A2의 1TB 드라이브에서 드라이브 베이 A1의 새로 설치된 2TB 드라이브로 데이터를 복사하려면 다음 명령을 입력하고 메시지가 표시되면 **y**를 입력합니다.

```
> request system raid copy from A2 to A1
```

2. 복사 프로세스의 상태를 보려면 다음 명령을 실행합니다.

```
> show system raid detail
```

어레이(이 예에서는 A1/A2)가 `Available`을 표시할 때까지 RAID 세부 출력을 보려면 이 명령을 계속 실행합니다.

이 시점에서 *A2* 드라이브는 드라이브 크기 불일치로 인해 *## ## ## #*으로 표시될 것입니다.

STEP 6 | RAID 1 어레이의 두 번째 드라이브를 2TB 드라이브로 업그레이드합니다.

1. RAID 1 어레이 구성을 위해 두 번째 1TB 드라이브(현재 예의 드라이브 베이 A2에서)를 제거합니다.

```
> request system raid remove A2
```

2. 새로 설치된 2TB 드라이브가 있는 캐리어를 드라이브 베이 A2에 삽입하고 RAID 1 어레이 구성에 추가합니다.

```
> request system raid add A2
```

시스템이 드라이브를 미러링하기 위해 A2에서 A1으로 데이터를 복사합니다.

3. 복사 프로세스의 상태를 보려면 다음 명령을 실행합니다.

```
> show system raid detail
```

어레이(이 예에서는 A1/A2)가 `Available`을 표시하고 두 드라이브 모두가 `active sync` 상태를 표시할 때까지 RAID 세부 출력을 계속 확인합니다.

```
Disk Pair A       Available Status         clean Disk id A1
     Present        model        : ST2000NX0253 size         :
 1907138 MB status       : active sync Disk id A2     Present
        model        : ST2000NX0253 size         : 1907138 MB
 status       : active sync
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 필요에 따라 추가 RAID 1 어레이용으로 드라이브를 업그레이드하십시오.

추가 RAID 1 어레이를 2TB 드라이브로 업그레이드하려면 해당하는 드라이브 지정자를 교체하여 이 절차를 반복하십시오. 예를 들어, A1을 B1으로 바꾸고 A2를 B2로 바꾸어 B1/B2 RAID 1 어레이의 드라이브를 업그레이드합니다.

다중 인터페이스를 사용하도록 Panorama 구성

대규모 네트워크에서는 리소스 사용량, 사용자 역할 및 보안 요구 사항에 따라 하위 네트워크를 분리하는 것과 관련된 네트워크 세분화를 구현하여 보안을 개선하고 혼잡을 줄일 수 있습니다. Panorama는 여러 M-시리즈 어플라이언스 인터페이스을(를) 사용하여 디바이스(방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터)를 관리하고 로그를 수집할 수 있도록 하여 네트워크 세분화를 지원합니다. 별도의 하위 네트워크에 있는 디바이스에 별도의 인터페이스를 할당할 수 있습니다.

여러 인터페이스를 사용하여 로그를 수집하면 로드 밸런싱의 이점도 제공되며, 이는 방화벽이 로그 수집기에 고속으로 로그를 포워딩하는 환경에서 특히 유용합니다. 수집기 그룹 로그 포워딩 기본 설정 목록에서 모든 로그 수집기로 포워딩 설정을 활성화하면 구성된 모든 구성된 인터페이스에서 로그가 전송됩니다. 그렇지 않으면 로그가 단일 인터페이스를 통해 포워딩되고 해당 인터페이스가 다운되면 다음으로 구성된 인터페이스를 통해 로그 포워딩이 계속됩니다. 예를 들어, 로그 포워딩을 위해 Eth1/1, Eth1/2 및 Eth1/3을 구성합니다. Eth1/1 인터페이스가 다운되는 경우 Eth1/2를 통해 로그 포워딩이 계속됩니다.

관리자는 MGT 인터페이스를 통해 Panorama에 액세스하고 관리하기 때문에 해당 인터페이스를 보호하는 것이 특히 중요합니다. MGT 인터페이스의 보안을 향상시키는 한 가지 방법은 Panorama 서비스를 다른 인터페이스로 오프로드하는 것입니다. 디바이스 관리 및 로그 수집 외에도 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터에 대한 소프트웨어 및 콘텐츠 업데이트 배포 및 Collector Group 통신을 오프로드할 수도 있습니다. 이러한 서비스를 오프로드하여 관리 트래픽을 위해 MGT 인터페이스를 예약하고 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터가 있는 하위 네트워크에서 분리된 보안 하위 네트워크에 할당할 수 있습니다.

- 네트워크 분할을 위한 다중 인터페이스 예
- 네트워크 분할을 위한 Panorama 구성

네트워크 분할을 위한 다중 인터페이스 예

Figure 1은(는) Panorama 모드 및 로그 수집기 모드에서 M-500 어플라이언스의 다중 인터페이스를 사용하는 배포를 보여줍니다. 이 예에서 인터페이스는 다음과 같이 네트워크 분할을 지원합니다.

- **Panorama** 관리 네트워크 - Panorama 웹 인터페이스, CLI 및 XML API를 무단 액세스로부터 보호하기 위해 Panorama의 MGT 인터페이스는 관리자만 액세스할 수 있는 하위 네트워크에 연결됩니다.
- 인터넷 - Panorama는 MGT 인터페이스를 사용하여 Palo Alto Networks Update Server와 같은 외부 서비스와 통신합니다.
- 경계 게이트웨이 및 데이터 센터 - Panorama는 별도의 인터페이스 쌍을 사용하여 이러한 각 하위 네트워크에서 방화벽 및 로그 수집기를 관리합니다. 방화벽 관리는 일반적으로 로그 수집기에 보고서 정보를 쿼리하는 것보다 적은 트래픽을 생성합니다. 따라서 Panorama는 방화벽 관리에 1Gbps 인터페이스(Eth1 및 Eth2)를 사용하고 Log Collector 쿼리 및 관리에 10Gbps 인터페이스(Eth4 및 Eth5)를 사용합니다. 각 로그 수집기는 MGT 인터페이스를 사용하여 쿼리에 응답하지만 방화벽에서 로그 수집과 관련된 더 많은 트래픽에 대해서는 Eth4 및 Eth5 인터페이스를 사용합니다.
- 소프트웨어 및 콘텐츠 업데이트 - 두 하위 네트워크의 방화벽 및 로그 수집기는 Panorama의 Eth3 인터페이스를 통해 소프트웨어 및 콘텐츠 업데이트를 검색합니다.

 ©2024 Palo Alto Networks, Inc.

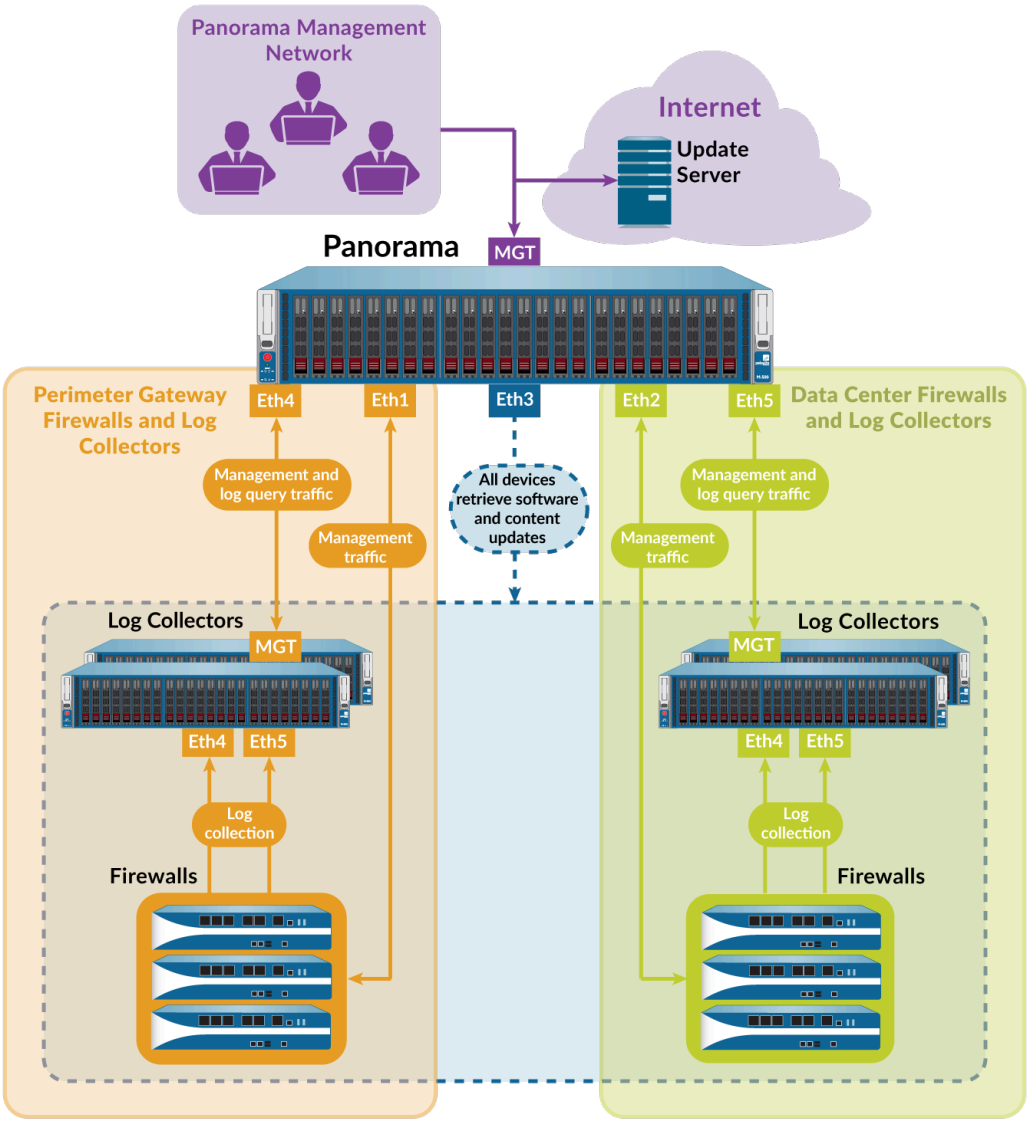


그림 **9:** 다중 **Panorama** 인터페이스

네트워크 분할을 위한 Panorama 구성

MGT 인터페이스에서 다른 인터페이스로 Panorama 서비스를 오프로드하려면 Panorama 관리 서버에서 인터페이스를 구성하여 시작합니다. 네트워크에 로그 트래픽이 많은 경우 M-500, M-600 및 M-700 어플라이언스의 Eth4 및 Eth5 인터페이스가 다른 인터페이스(1Gbps)보다 높은 처리량(10Gbps)을 지원한다는 점을 기억하십시오. 그런 다음 Panorama의 특정 인터페이스와 연결하도록 각 하위 네트워크의 로그 수집기를 구성합니다. 각 Log Collector에 대해 Collector Group 통신을 위한 인터페이스와 방화벽에서 로그를 수집하기 위한 하나 이상의 인터페이스도 선택합니다. 마지막으로 Panorama의 인터페이스와 연결하도록 각 하위 네트워크의 방화벽을 구성합니다.

10GB 인터페이스가 있는 *Log Collector* 모드에서 *M*-시리즈 기기를 구성하는 경우 *10GB* 인터페이스가 *Up*으로 표시되도록 이 전체 구성 절차를 완료해야 합니다.

©2024 Palo Alto Networks, Inc.

*Palo Alto Networks*는 *IP* 주소, 넷마스크*(IPv4*의 경우*)* 또는 접두사 길이*(IPv6*의 경우*)* 및 *MGT* 인터페이스의 기본 게이트웨이를 지정할 것을 권장합니다. 이러한 설정*(*예*:* 기본 게이트웨이*)* 중 하나를 생략하면 향후 구성 변경을 위해 콘솔 포트를 통해서만 *M-Series* 어플라이언스에 액세스할 수 있습니다.

여러 인터페이스를 사용하도록 Panorama 및 전용 로그 수집기를 구성하려면 다음 단계를 수행하십시오.

STEP 1 | Panorama 어플라이언스 및 방화벽이 여러 인터페이스를 지원하고 필수 소프트웨어 버전 및 구성이 있는지 확인합니다.

- M-시리즈 어플라이언스는 업데이트 배포에 별도의 인터페이스를 사용하고 디바이스 관리 및 로그 수집에 여러 인터페이스를 사용하려면 Panorama 8.0 이상의 버전을 실행해야 합니다. M-200 및 M-600 어플라이언스는 Panorama 8.1 이상을 실행해야 하고 M-300 및 M-700은 Panorama 11.1 이상을 실행해야 합니다. ESXi, vCloud, Air, Hyper-V 및 KVM에 배포된 Panorama 어플라이언스는 Panorama 8.1 이상의 버전을 실행해야 합니다.
- Panorama 또는 Log Collector를 가상 어플라이언스로 배포한 경우 Panorama 가상 어플라이언스에 대해 지원되는 인터페이스를 확인하십시오.
- 로그 수집 또는 수집기 그룹 통신에 별도의 인터페이스를 사용하려면 M-시리즈 기기에서 Panorama 6.1 이상의 버전을 실행해야 합니다.
- 각 Panorama 관리 서버의 초기 구성이 완료되었습니다. 여기에는 MGT 인터페이스의 구성이 포함됩니다.

  Panorama MGT 인터페이스에 대한 *IPv6 IP* 주소를 구성하려면 *IPv6 IP* 주소를 사용하여 *Panorama*를 성공적으로 구성하도록 *IPv4* 및 *IPv6*을 모두 구성해야 합니다. *Panorama*는 *IPv6 IP* 주소만으로 *MGT* 인터페이스 구성을 지원하지 않습니다.
- 로그 수집기 및 수집기 그룹이 구성됩니다. 여기에는 로그 수집기의 MGT 인터페이스 구성이 포함됩니다.

  로그 수집기의 *MGT* 인터페이스에 대한 *IPv6 IP* 주소를 구성하려면 *IPv6 IP* 주소를 사용하여 *Panorama*를 성공적으로 구성하도록 *IPv4* 및 *IPv6*를 모두 구성해야 합니다. *Panorama*는 *IPv6 IP* 주소만으로 *MGT* 인터페이스 구성을 지원하지 않습니다.
- 방화벽의 초기 구성이 완료되고 Panorama에 관리 디바이스로 방화벽을 추가했으며 각 하위 네트워크의 방화벽이 별도의 템플릿에 할당되었습니다.
- WildFire 어플라이언스의 초기 구성이 완료되었으며 WildFire 어플라이언스를 Panorama에 관리 디바이스로 추가했습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 단독(비 HA) 또는 활성(HA) Panorama 관리 서버에서 인터페이스를 구성합니다.

MGT 인터페이스는 초기 *Panorama* 구성 중에 구성되었으므로 다시 구성할 필요가 없습니다.

각 인터페이스에 대해 다음 단계를 수행합니다.

1. 단독(비 HA) 또는 활성(HA) Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 인터페이스를 선택합니다.
3. 인터페이스 이름을 클릭하여 인터페이스를 편집합니다.
4. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
5. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 둘 다를 구성합니다.
   - IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
6. 인터페이스가 지원하는 서비스를 선택하십시오.
   - 디바이스 관리 및 디바이스 로그 수집 - 방화벽, 로그 수집기, WildFire 기기 및 기기 클러스터를 관리하고, 로그 수집기가 생성하는 로그를 수집하고, 로그 수집기에 보고서 정보를 쿼리합니다. 분할된 네트워크를 지원하기 위해 여러 인터페이스에서 이러한 서비스를 활성화할 수 있습니다.
   - 수집기 그룹 통신 - Panorama가 모든 하위 네트워크에서 관리하는 수집기 그룹과 통신합니다.
   - 디바이스 배포 - 모든 하위 네트워크에 걸쳐 관리 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터에 소프트웨어 및 콘텐츠 업데이트를 배포합니다.
7. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
8. **Commit** > **Panorama**에 커밋을 클릭하고 변경 사항을 커밋합니다.
9. **Commit** > 디바이스에 푸시을 클릭하고 수정한 로그 수집기가 포함된 수집기 그룹에 변경 사항을 푸시합니다.

STEP 3 | (HA만 해당) 패시브 Panorama 관리 서버에서 인터페이스를 구성합니다.

1. 활성 Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리형 수집기를 선택하고 수동 HA 피어를 선택합니다.
3. 인터페이스를 선택하고 편집할 인터페이스를 클릭합니다.
4. 인터페이스 활성화 확인란을 선택하여 인터페이스를 활성화합니다.
5. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 둘 다를 구성합니다.
   - IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
6. 인터페이스가 지원하는 서비스를 선택하십시오.
   - 디바이스 관리 및 디바이스 로그 수집 - 방화벽, 로그 수집기, WildFire 기기 및 기기 클러스터를 관리하고, 로그 수집기가 생성하는 로그를 수집하고, 로그 수집기에 보고서 정보를 쿼리합

 ©2024 Palo Alto Networks, Inc.

니다. 분할된 네트워크를 지원하기 위해 여러 인터페이스에서 이러한 서비스를 활성화할 수 있습니다.

- 수집기 그룹 통신 - Panorama가 모든 하위 네트워크에서 관리하는 수집기 그룹과 통신합니다.
- 디바이스 배포 - 모든 하위 네트워크에 걸쳐 관리 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터에 소프트웨어 및 콘텐츠 업데이트를 배포합니다.

7. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
8. 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 수정한 패시브 HA 피어가 포함된 수집기 그룹에 변경 사항을 푸시합니다.

STEP 4 | Panorama 인터페이스와 연결하도록 각 Log Collector를 구성합니다.

분할된 네트워크를 지원하기 위해 각 하위 네트워크의 로그 수집기를 별도의 Panorama 인터페이스에 연결할 수 있습니다. 인터페이스에는 이전 단계에서 설명한 대로 디바이스 관리 및 디바이스 로그 수집이 활성화되어 있어야 합니다.

1. 단독(비 HA) 또는 활성(HA) Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
3. **Panorama Server IP** 필드에 단독(비 HA) 또는 활성(HA) Panorama에 있는 인터페이스의 IP 주소를 입력합니다.
4. (HA만 해당) **Panorama Server IP 2** 필드에 활성 Panorama에서 페일오버가 발생할 경우 디바이스 관리 및 디바이스 로그 수집을 지원할 수동 Panorama 인터페이스의 IP 주소를 입력합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.
6. 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 수정한 로그 수집기가 포함된 수집기 그룹에 변경 사항을 푸시합니다.
7. 각 전용 로그 수집기에서 다음 단계를 수행합니다.
   1. PuTTY와 같은 에뮬레이션 소프트웨어를 사용하여 Log Collector CLI에 액세스하여 MGT 인터페이스 IP 주소를 사용하여 Log Collector에 대한 SSH 세션을 엽니다. 메시지가 표시되면 Panorama 관리자 자격 증명을 사용하여 로그인합니다.
   2. 다음 명령을 실행합니다. 여기서 *<IPaddress1>*은(는) 단독(비 HA) 또는 활성(HA) Panorama용이고 *<IPaddress2>*은(는) 수동 Panorama(해당되는 경우)용입니다.

```
> configure # set deviceconfig system panorama-
server <IPaddress1> panorama-server-2 <IPaddress2> # commit
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (HA만 해당) 활성 Panorama가 페일오버되는 경우 업데이트를 배포하도록 수동 Panorama 관리 서버의 인터페이스를 구성합니다.

1. 패시브 Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 인터페이스를 선택합니다.
3. 인터페이스 이름을 클릭하여 인터페이스를 편집합니다.
4. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
5. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 둘 다를 구성합니다.
   - IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
6. 디바이스 배포를 선택합니다.
7. 확인을 클릭하여 변경 사항을 저장합니다.
8. **Commit** > **Panorama**에 커밋을 클릭하고 변경 사항을 커밋합니다.

STEP 6 | Log Collector가 방화벽에서 로그를 수집하고 다른 Log Collector와 통신하는 데 사용할 인터페이스를 구성합니다.

MGT 인터페이스는 *Log Collector*의 초기 구성 중에 구성되었으므로 다시 구성할 필요가 없습니다.

1. 단독(비 HA) 또는 활성(HA) Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
3. 인터페이스를 선택하고 각 인터페이스에 대해 다음 단계를 수행합니다.
   1. 인터페이스 이름을 클릭하여 해당 인터페이스를 편집합니다.
   2. 인터페이스를 활성화하려면 *<interface-name>*을(를) 선택합니다.
   3. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 둘 다를 구성하십시오.

      IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   4. 인터페이스가 지원하는 기능을 선택하십시오.

      디바이스 로그 수집 - 방화벽에서 로그를 수집합니다. 여러 인터페이스가 이 기능을 수행할 수 있도록 하여 로깅 트래픽의 부하를 분산할 수 있습니다.

      수집기 그룹 통신 - 수집기 그룹의 다른 로그 수집기와 통신합니다.
   5. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
4. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.
5. 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 수정한 로그 수집기가 포함된 수집기 그룹에 변경 사항을 푸시합니다.
6. **Panorama** > 관리형 수집기를 선택하여 로그 수집기가 Panorama와 동기화되고 연결되었는지 확인합니다.

   구성 상태 열에는 `InSync`가 표시되어야 하고 런타임 상태 열에는 ###이 표시되어야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 인터페이스와 연결하도록 방화벽을 구성합니다.

분할된 네트워크를 지원하기 위해 각 하위 네트워크의 방화벽을 별도의 Panorama 인터페이스에 연결할 수 있습니다. 인터페이스에는 디바이스 관리 및 디바이스 로그 수집 이 활성화되어 있어야 합니다. 이 단계에서는 별도의 템플릿을 사용하여 별도의 하위 네트워크에 방화벽을 구성한다고 가정합니다.



이 예제 배포에서 *Panorama*는 이러한 인터페이스를 사용하여 방화벽을 관리하지만 방화벽 로그를 수집하지 않습니다. 수집기 그룹을 구성할 때 방화벽 로그를 수집할 전용 로그 수집기를 지정합니다.

1. 단독(비 HA) 또는 활성(HA) Panorama 관리 서버의 Panorama 웹 인터페이스에 로그인.
2. Panorama에서 디바이스 > 설정 > 관리를 선택하고 템플릿을 선택한 다음 Panorama 설정을 편집합니다.
3. 첫 번째 **Panorama Servers** 필드에 단독(비 HA) 또는 활성(HA) Panorama에 있는 인터페이스의 IP 주소를 입력합니다.
4. (HA만 해당) 두 번째 **Panorama Servers** 필드에 페일오버가 발생할 경우 디바이스 관리를 지원할 패시브 Panorama 인터페이스의 IP 주소를 입력합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.
6. 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 템플릿 변경 사항을 방화벽에 푸시합니다.
7. **Panorama** > 관리형 디바이스를 선택하여 방화벽이 Panorama와 동기화되고 연결되었는지 확인합니다.

   디바이스 상태 열에 ###이 표시되어야 합니다. 공유 정책 및 템플릿 열에 `InSync`가 표시되어야 합니다.

©2024 Palo Alto Networks, Inc.

Panorama 등록 및 라이선스 설치

중앙 집중식 관리, 로깅 및 보고를 위해 Panorama를 사용하려면 먼저 Panorama 디바이스 관리 및 지원 라이선스를 등록, 활성화 및 검색해야 합니다. Panorama의 모든 인스턴스에는 방화벽을 관리하고 지원을 받을 수 있는 유효한 라이선스가 필요합니다. 방화벽 디바이스 관리 라이선스는 Panorama가 관리할 수 있는 최대 방화벽 수를 적용합니다. 이 라이선스는 각 방화벽의 가상 시스템 수가 아니라 방화벽 일련번호를 기반으로 합니다. 지원 라이선스는 Panorama 소프트웨어 업데이트 및 동적 콘텐츠 업데이트를 활성화합니다(예: 최신 애플리케이션 및 위협 서명의 경우). 또한 AWS 및 Azure의 Panorama 가상 어플라이언스는 Palo Alto Networks에서 구매해야 하며 AWS 또는 Azure 마켓플레이스에서 구매할 수 없습니다.

Panorama 가상 어플라이언스를 PAN-OS 8.1로 업그레이드한 후 용량 라이선스가 성공적으로 설치되지 않았거나 Panorama에서 관리하는 총 방화벽 수가 디바이스 관리 라이선스를 초과하는 경우 메시지가 표시됩니다. 라이선스가 설치되지 않은 경우 업그레이드 날짜로부터 180일 이내에 유효한 디바이스 관리 라이선스를 설치할 수 있습니다. 관리되는 방화벽의 수가 디바이스 관리 라이선스를 초과하는 경우 디바이스 관리 라이선스 요구 사항을 충족하기 위해 방화벽을 삭제하거나 디바이스 관리 라이선스를 업그레이드할 수 있도록 180일이 주어집니다. 업그레이드 후 180일 이내에 유효한 디바이스 관리 라이선스가 설치되어 있지 않거나 기존 디바이스 관리 라이선스 제한이 충족되지 않으면 모든 커밋이 실패합니다. 디바이스 관리 라이선스를 구입하려면 Palo Alto Networks 영업 담당자 또는 공인 대리점에 문의하십시오.

클라우드 기반 Strata Logging Service를 사용하려면 방화벽 관리 라이선스와 프리미엄 지원 라이선스 외에 Strata Logging Service 라이선스가 필요합니다. 라이선스를 구매하려면 Palo Alto Networks 시스템 엔지니어나 리셀러에게 문의하십시오.



Panorama 가상 어플라이언스에서 방화벽 관리를 위한 평가판 라이선스를 실행 중이고 구입한 *Panorama* 라이선스를 적용하려면 Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 Panorama 등록 및 방화벽 관리 라이선스 활성화/검색 작업을 수행하십시오.

- Panorama 등록
- Panorama 지원 라이선스 활성화
- Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색
- Panorama Virtual Appliance가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스 활성화/검색
- M-시리즈 어플라이언스에서 방화벽 관리 라이선스 활성화/검색

Panorama 등록

©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 일련번호 또는 인증 코드를 기록하고 판매 주문 번호 또는 고객 ID를 기록합니다.

인증 코드, 판매 주문 번호 또는 고객 ID는 Panorama를 주문할 때 Palo Alto Networks 고객 서비스에서 보낸 주문 이행 이메일을 참조하십시오.

일련번호의 경우 위치는 모델에 따라 다릅니다.

- M-시리즈 어플라이언스 - Panorama 웹 인터페이스에 로그인하고 대시보드 탭의 일반 정보 섹션에 일련번호 값을 기록합니다.
- Panorama 가상 어플라이언스 - 주문 이행 이메일을 참조하거나 VM Flex 라이선스를 사용하여 Panorama를 프로비저닝할 때 생성된 일련 번호를 참조하십시오.



VM Flex 라이선스를 사용하여 일련 번호를 할당하면 *Panorama* 가상 어플라이언스가 자동으로 등록됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Palo Alto Networks 고객 지원 포털(CSP)에서 Panorama를 등록하십시오.

단계는 Palo Alto Networks CSP에 대한 로그인이 이미 있는지의 여부에 따라 다릅니다.

- 등록하는 첫 번째 Palo Alto Networks 어플라이언스이고 아직 CSP 로그인이 없는 경우:
  1. Palo Alto Networks CSP로 이동합니다.
  2. 내 계정 생성을 클릭합니다.
  3. 이메일 주소를 입력하고 reCAPTCHA 프롬프트에 응답합니다.
  4. reCAPTCHA 프롬프트에 성공적으로 응답한 후 제출을 클릭합니다.
  5. 일련 번호 또는 인증 코드를 사용하여 디바이스 등록을 선택하고제출을 클릭합니다.
  6. 연락처 세부 정보 만들기 및 사용자 **ID** 및 암호 만들기 섹션의 필드를 완료합니다.
  7. Panorama 디바이스 일련번호 또는 인증 코드를 입력합니다.
  8. 판매 주문 번호 또는 고객 **ID**를 입력합니다.
  9. reCAPTCHA 프롬프트에 응답합니다.
  10. reCAPTCHA 프롬프트에 성공적으로 응답한 후 제출을 클릭합니다.
- 이미 CSP 로그인이 있는 경우:
  1. Palo Alto Networks CSP에 로그인합니다.
  2. 자산 > 디바이스 > 새 디바이스 등록을 클릭합니다.

     CSP 지원 홈에서디바이스를 등록할 수도 있습니다.
  3. 일련번호를 사용하여 디바이스 등록을 선택한 후 다음을 클릭합니다.
  4. Panorama 일련번호를 입력합니다.
  5. 디바이스 이름을 입력하여 Panorama를 검색하고 식별하는 이름을 적용합니다.
  6. (선택 사항)디바이스 태그를 선택한 다른 디바이스와 함께 Panorama를 그룹화하려면 디바이스 태그를 선택합니다.

     디바이스 태그는 Panorama를 등록할 때 선택하기 전에 먼저 계정 수준(자산 > 디바이스 > 디바이스 태그)에서 생성되어야 합니다.
  7. Panorama 관리 서버가 인터넷에 연결되어 있지 않으면 디바이스가 오프라인으로 사용됩니다를 체크하고 **OS** 릴리스 버전을 선택합니다.
  8. 4시간 RMA를 구매한 경우 필수 위치 정보(별표로 표시)를 입력합니다.
  9. **EULA**에 동의하고 제출합니다.

     등록 완료 메시지가 표시되면 기기 등록 대화상자를 닫습니다.

Panorama 지원 라이선스 활성화

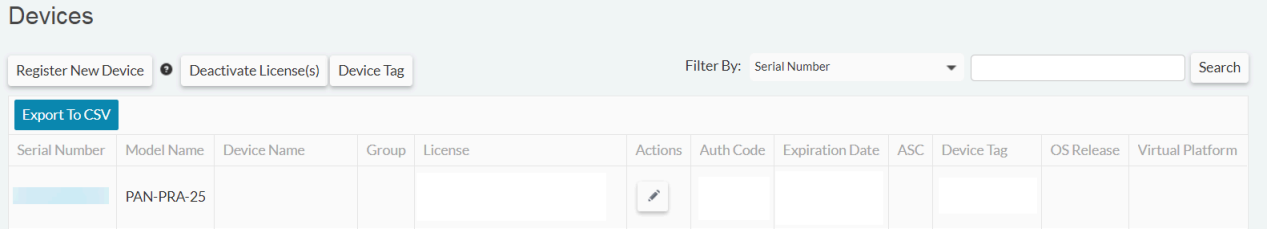
Panorama M-Series 어플라이언스 또는 Panorama 가상 어플라이언스에서 Panorama 지원 라이선스를 활성화하기 전에 Panorama를 등록해야 합니다.

 ©2024 Palo Alto Networks, Inc.

지원 라이선스가 만료되더라도 *Panorama*는 여전히 방화벽을 관리하고 로그를 수집할 수 있지만 소프트웨어 및 콘텐츠 업데이트는 사용할 수 없습니다. *Panorama*의 소프트웨어 및 콘텐츠 버전은 관리되는 방화벽의 버전 이상이어야 합니다. 그렇지 않으면 오류가 발생합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.

STEP 1 | Palo Alto Networks 고객 지원 포털에 로그인하여 인증 코드를 활성화합니다.

1. 자산 > 디바이스를 선택하고 Panorama 일련번호를 입력하여 일련번호로 필터링합니다.



2. 작업 열에서 연필 아이콘을 선택하고 인증 코드 활성화를 선택하고 지원 라이선스 인증 코드를 입력하고 동의 및 제출을 클릭합니다.

STEP 2 | Panorama 웹 인터페이스에 로그인하고 인증 코드를 사용하여**Panorama** > **Support** > 기능 활성화를 선택합니다.

STEP 3 | 인증 코드를 입력하고 확인을 클릭합니다.

STEP 4 | 구독이 활성화되었는지 확인합니다. 페이지의 지원 섹션에서 세부 정보(예: 만료 날짜, 지원 수준 및 설명)를 확인합니다.

Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색

Panorama에서 디바이스를 관리하려면 PAN-OS에서 생성한 방화벽 관리 라이선스를 활성화해야 합니다. 활성화하는 디바이스 관리 라이선스에 따라 Panorama가 관리할 수 있는 디바이스의 수가 결정됩니다. Log Collector 및 WildFire 어플라이언스는 관리되는 디바이스로 취급되지 않으며 디바이스 관리 라이선스에 의해 할당된 디바이스 수에 포함되지 않습니다.

Panorama 가상 어플라이언스에서 방화벽 관리 라이선스를 활성화하고 검색하기 전에 Panorama를 등록해야 합니다. 평가판 라이선스를 실행 중이고 구매한 라이선스를 적용하려면 구매한 라이선스를 등록하고 활성화/검색해야 합니다. 또한 Panorama의 일련번호를 평가 일련번호에서 생산 일련번호로 변경해야 합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.

STEP 3 | Panorama 일련번호(주문 이행 이메일에 포함)를 입력하고 확인을 클릭합니다.

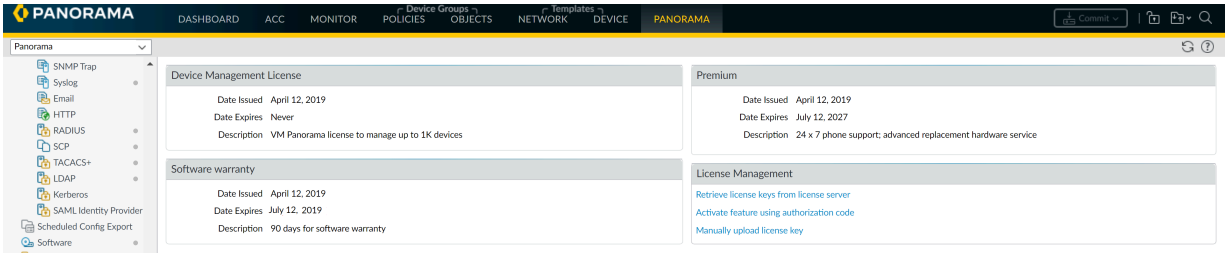
 ©2024 Palo Alto Networks, Inc.

STEP 4 | 방화벽 관리 라이선스를 활성화하거나 검색하려면 **Panorama** > 라이선스를 선택합니다.

- 라이선스 서버에서 라이선스 키 검색 - Panorama는 Panorama 업데이트 서버에서 방화벽 관리 라이선스를 자동으로 검색하고 활성화합니다.
- 인증 코드를 사용하여 기능 활성화 - 방화벽 관리 라이선스 인증 코드를 입력하고 확인을 클릭하여 라이선스를 활성화합니다. 승인 코드는 주문 처리 이메일에서 또는 Panorama 관리 서버를 찾아 Palo Alto Networks 고객 지원 웹 사이트에 로그인하여 얻을 수 있습니다.
- 수동으로 라이선스 키 업로드 - Palo Alto Networks 고객 지원 웹 사이트에 로그인하고 Panorama 관리 서버를 찾은 다음 방화벽 관리 라이선스 키를 로컬 디바이스에 다운로드합니다. 라이선스 키를 다운로드한 후 파일 선택을 클릭하여 라이선스 키를 선택하고 확인을 클릭하십시오.

STEP 5 | 방화벽 관리 라이선스가 활성화되어 있는지 확인합니다.

이제 디바이스 관리 라이선스 섹션이 나타나 라이선스가 발행된 날짜, 라이선스 만료 시간 및 방화벽 관리 라이선스에 대한 설명을 표시합니다.



Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스 활성화/검색

Panorama 가상 어플라이언스에서 방화벽 관리 라이선스를 활성화하고 검색하기 전에 Panorama를 등록해야 합니다. Panorama에서 디바이스를 관리하려면 디바이스 관리 라이선스를 활성화해야 합니다. 활성화하는 디바이스 관리 라이선스에 따라 Panorama가 관리할 수 있는 디바이스의 수가 결정됩니다. Log Collectors 및 WildFire 어플라이언스는 관리되는 디바이스로 취급되지 않으며 디바이스 관리 라이선스에 의해 할당된 디바이스 수에 포함되지 않습니다. 평가판 라이선스를 실행 중이고 구매한 라이선스를 적용하려면 구매한 라이선스를 등록하고 활성화/검색해야 합니다.

PAN-OS 8.1로 업그레이드한 후 Panorama 재부팅이 완료되면 Panorama 웹 인터페이스에 처음 로그인할 때 유효한 Panorama 관리 라이선스를 검색하라는 메시지가 표시됩니다. Panorama 가상 어플라이언스가 오프라인이거나 Palo Alto Networks 업데이트 서버에 연결할 수 없는 경우 유효한 관리 라이선스를 활성화하거나 검색하려면 Panorama 가상 어플라이언스에 대한 관련 어플라이언스 정보를 가져와서 고객 지원 웹 사이트에 업로드해야 합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | (초기 배포에만 해당) Panorama 일련번호를 입력합니다.

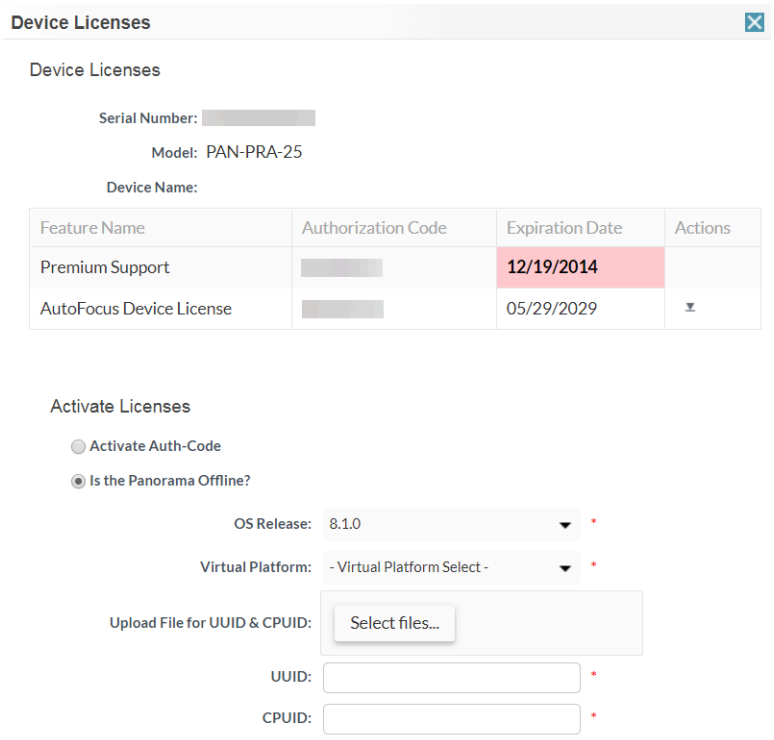
1. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
2. Panorama 일련번호(주문 이행 이메일에 포함)를 입력하고 확인을 클릭합니다.
3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama 가상 어플라이언스 정보를 고객 지원 웹사이트에 업로드합니다.

1. 관리 라이선스 검색 대화 상자에서 여기 링크를 클릭하여 **UUID**, **CPUID**, Panorama 버전 및 가상 플랫폼 정보를 수집합니다. 다운로드 링크를 클릭하여 고객 지원 포털에 업로드할 수 있는 필수 Panorama 정보의 XML 파일을 다운로드합니다.

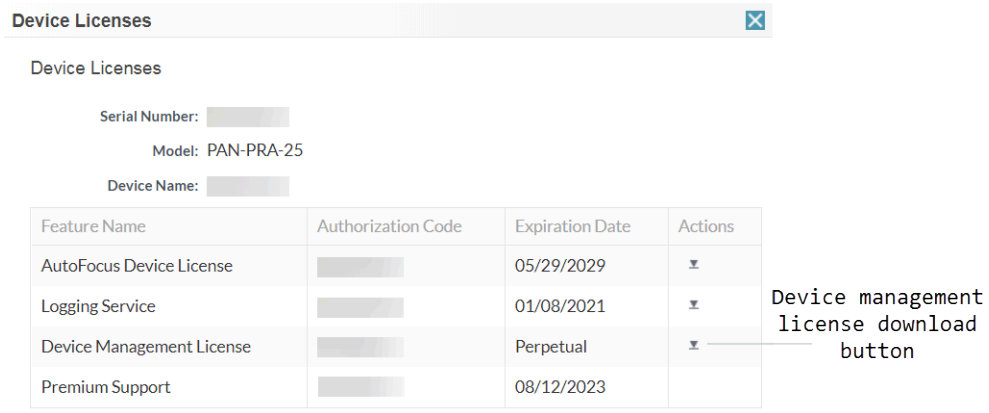
   초기 배포 시 대화를 보려면 웹 인터페이스에서 로그아웃했다가 다시 로그인해야 할 수 있습니다.
2. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
3. 오른쪽 상단에서 지원 받기를 클릭합니다.
4. 자산 > 디바이스를 선택하고 Panorama 가상 어플라이언스를 찾은 다음 작업 열에서 편집 아이콘()을 클릭합니다.
5. **Panorama**가 오프라인입니까**?**를 선택하십시오. 2단계에서 수집한 Panorama 정보를 입력하거나 파일 선택**...**을 클릭하여 다운로드한 XML 파일을 업로드합니다.
6. EULA에 동의하고 제출합니다.



 ©2024 Palo Alto Networks, Inc.

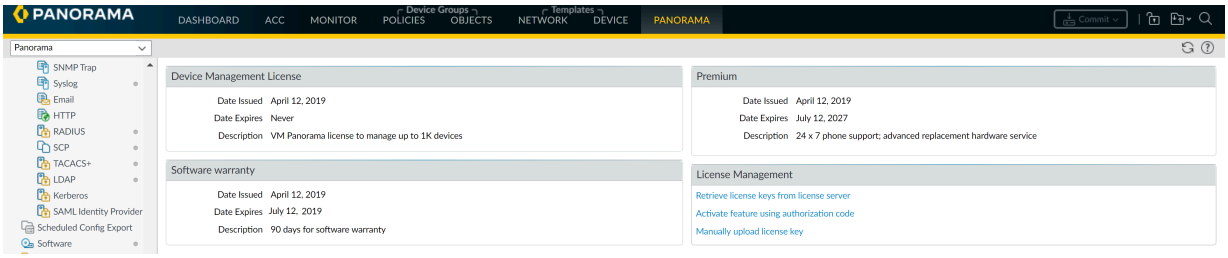
STEP 4 | 디바이스 관리 라이선스를 설치합니다.

1. 작업 열에서 디바이스 관리 라이선스를 다운로드합니다.



2. Panorama 웹 인터페이스에서**Panorama** > 라이선스를 클릭하고 라이선스 키를 수동으로 업로드합니다.
3. 파일 선택을 클릭하고 다운로드한 디바이스 관리 라이선스 키를 찾은 다음 확인을 클릭합니다.

STEP 5 | 디바이스 관리 라이선스가 라이선스 정보와 함께 표시되는지 확인하여 디바이스 관리 라이선스가 성공적으로 업로드되었는지 확인하십시오.



M-시리즈 어플라이언스에서 방화벽 관리 라이선스 활성화/검색

Panorama에서 디바이스를 관리하려면 용량 라이선스를 활성화해야 합니다. 용량 라이선스는 Panorama가 관리할 수 있는 디바이스의 수를 결정합니다. Log Collector 및 WildFire 어플라이언스는 관리되는 디바이스로 취급되지 않으며 용량 라이선스에 의해 할당된 디바이스 수에 포함되지 않습니다.

M-시리즈 어플라이언스에서 Panorama 방화벽 관리 라이선스를 활성화하고 검색하기 전에:

- Panorama를 등록합니다.
- 구매한 제품/구독에 대한 인증 코드를 찾습니다. 주문을 하면 Palo Alto Networks 고객 서비스에서 구매와 관련된 인증 코드가 나열된 이메일을 보냈습니다. 이 이메일을 찾을 수 없는 경우 계속하기 전에 Palo Alto Networks 고객 지원에 연락하여 코드를 받으십시오.

라이선스를 활성화하고 검색하면 **Panorama** > 라이선스 페이지에 관련 발급 날짜, 만료 날짜 및 라이선스로 Panorama가 관리할 수 있는 방화벽 수가 표시됩니다.

라이선스를 활성화하고 검색하기 위한 옵션은 다음과 같습니다.

 ©2024 Palo Alto Networks, Inc.

- 웹 인터페이스를 사용하여 라이선스를 활성화하고 검색합니다.

  Panorama가 Palo Alto Networks 업데이트 서버에 연결할 준비가 되었지만(M-Series Appliance의 초기 구성 수행 작업을 완료함) Palo Alto Networks 고객 지원 웹 사이트에서 라이선스를 활성화하지 않은 경우 이 옵션을 선택하십시오.

  1. **Panorama** > 라이선스를 선택하고 인증 코드를 사용하여 기능 활성화를 클릭합니다.
  2. 인증 코드를 입력하고 확인을 클릭합니다. Panorama는 라이선스를 검색하고 활성화합니다.

- 라이선스 서버에서 라이선스 키를 검색합니다.

  Panorama가 업데이트 서버에 연결할 준비가 되지 않은 경우(예: 초기 M-Series 어플라이언스 설정을 완료하지 않은 경우) 지원 웹사이트에서 라이선스를 활성화하여 Panorama가 연결할 준비가 되면 다음을 수행할 수 있습니다. 웹 인터페이스를 사용하여 활성화된 라이선스를 검색합니다. 활성화된 라이선스를 검색하는 프로세스는 검색 및 활성화하는 프로세스보다 빠릅니다.

  1. Palo Alto Networks 고객 지원 웹 사이트에서 라이선스를 활성화하십시오.
     1. 인터넷에 액세스할 수 있는 호스트에서 웹 브라우저를 사용하여 Palo Alto Networks 고객 지원 웹 사이트에 액세스하고 로그인합니다.
     2. **Assets** > **Devices**를 선택하고 M-Series 어플라이언스를 찾은 다음 작업 열에서 편집 아이콘()을 클릭합니다.
     3. 인증 코드 활성화를 선택하고 인증 코드를 입력한 다음 동의 및 제출을 클릭하여 라이선스를 활성화합니다.
  2. 업데이트 서버에 연결하도록 Panorama를 구성합니다. M-시리즈 어플라이언스의 초기 구성 수행을 참조하십시오.
  3. **Panorama** > 라이선스를 선택하고 라이선스 서버에서 라이선스 키 검색을 클릭합니다. Panorama는 활성화된 라이선스를 검색합니다.

©2024 Palo Alto Networks, Inc.

- 호스트에서 Panorama로 라이선스를 수동으로 업로드합니다. Panorama는 해당 호스트에 액세스할 수 있어야 합니다.

  Panorama가 설정되었지만(M-시리즈 어플라이언스의 초기 구성 수행 작업을 완료함) 업데이트 서버에 연결되어 있지 않은 경우 지원 웹사이트에서 라이선스를 활성화하고 서버를 업데이트한 다음 Panorama에 업로드합니다.

  1. Palo Alto Networks 고객 지원 웹 사이트에서 라이선스를 활성화하고 다운로드하십시오.
     1. 인터넷에 액세스할 수 있는 호스트에서 웹 브라우저를 사용하여 Palo Alto Networks 고객 지원 웹 사이트에 액세스하고 로그인합니다.
     2. **Assets** > **Devices**를 선택하고 M-Series 어플라이언스를 찾은 다음 작업 열에서 편집 아이콘()을 클릭합니다.
     3. 인증 코드 활성화를 선택하고 인증 코드를 입력한 다음 동의 및 제출을 클릭하여 라이선스를 활성화합니다.
     4. 작업 열에서 다운로드 아이콘을 클릭하고 라이선스 키 파일을 호스트에 저장합니다.
  2. Panorama 웹 인터페이스에서 **Panorama** > **Licenses**를 선택하고 수동으로 라이선스 키 업로드를 클릭한 다음 찾아보기를 클릭합니다.
  3. 호스트에 다운로드한 키 파일을 선택하고 열기를 클릭합니다.
  4. 확인을 클릭하여 활성화된 라이선스 키를 업로드합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 디바이스 인증서 설치

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• NGFW (Managed by Panorama)	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스 ❑ 아웃바운드 인터넷 액세스 ❑ 다음 사용자 역할 중 하나를 가진 고객 지원 포털(CSP) 계정: 수퍼유저, 표준 사용자, 제한된 사용자, 위협 연구원, AutoFocus 평가판 역할, 그룹 수퍼유저, 그룹 표준 사용자, 그룹 제한된 사용자, 그룹 위협 연구원, 승인된 지원 센터(ASC) 사용자 및 ASC 전체 서비스 사용자 ❑ Panorama 수퍼유저 역할

하나 이상의 클라우드 서비스를 사용하려면 Panorama™ 관리 서버에 디바이스 인증서를 설치해야 합니다. 디바이스 인증서는 한 번만 설치하면 됩니다. 디바이스 인증서의 수명은 90일입니다. 방화벽은 인증서가 만료되기 15일 전에 디바이스 인증서를 다시 설치합니다. Panorama가 자체적으로 디바이스 인증서를 다시 설치할 수 없는 경우 수동으로 만료된 디바이스 인증서를 복원해야 할 수도 있습니다.

디바이스 인증서를 성공적으로 설치하려면 Panorama에 아웃바운드 인터넷 연결이 있어야 하며 네트워크에서 다음 정규화된 도메인 이름(FQDN) 및 포트를 허용해야 합니다.

FQDN	포트
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 및 TCP 443

M-300 및 *M-700* 어플라이언스는 초기 등록 프로세스 중 *Palo Alto Networks CSP*에 처음 연결할 때 디바이스 인증서를 자동으로 설치합니다. 이러한 *M-Series* 어플라이언스의 경우 디바이스 인증서를 수동으로 설치할 필요가 없습니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 일회용 암호(OTP)를 생성합니다.

OTP 수명은 *60*분이며 *60*분 수명 내에 사용하지 않으면 만료됩니다.

*Panorama*는 *CSP*에서 *OTP* 검색을 한 번만 시도할 수 있습니다. 어떤 이유로든 *Panorama*가 *OTP*를 가져오는 데 실패하면 *OTP*가 만료되어 새 *OTP*를 생성해야 합니다.

1. OTP 생성 권한이 있는 사용자 역할로 고객 지원 포털에 로그인합니다.
2. 제품 > 디바이스 인증서를 선택하고 **OTP** 생성을 선택합니다.
3. 디바이스 유형에서 **Panorama** 관리형 방화벽용 **OTP** 생성을 선택하고 다음을 클릭합니다.
4. **Panorama** 디바이스 일련번호를 선택하고 **OTP** 생성을 선택합니다.
5. **OTP**를 생성하고 OTP를 복사합니다.

STEP 2 | 수퍼유저로 Panorama 웹 인터페이스에 로그인합니다.

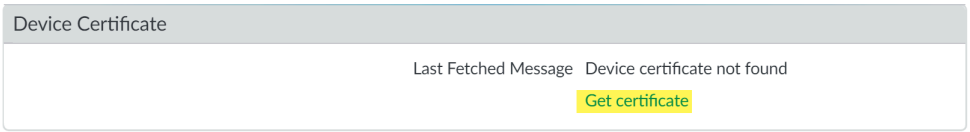
Panorama에 디바이스 인증서를 설치하는 데 사용되는 OTP를 적용하려면 수퍼유저 액세스 권한이 있는 Panorama 관리자가 필요합니다.

STEP 3 | NTP(네트워크 시간 프로토콜) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. **Panorama** > 설정 > 서비스를 선택합니다.
2. **NTP**를 선택하고 기본 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
3. (선택 사항) 보조 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
4. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) - NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID 입력(1-65534)
     - 알고리즘 - NTP 인증(**MDS** 또는 **SHA1**)에 사용할 알고리즘을 선택합니다.
5. 확인을 클릭하여 구성 변경 사항을 저장합니다.
6. 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 4 | **Panorama** > 설정 > 관리 > 디바이스 인증서 설정 및 인증서 가져오기를 선택합니다.



STEP 5 | 생성한 일회용 암호를 입력하고 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Panorama가 인증서를 성공적으로 검색하고 설치합니다.

Device Certificate	
Current Device Certificate Status	Valid
Not Valid Before	2020/04/01 21:52:28 PDT
Not Valid After	2020/06/30 21:52:28 PDT
Last Fetched Message	Successfully fetched device certificate
Last Fetched Status	success
Last Fetched Timestamp	2020/04/01 22:02:28 PDT

©2024 Palo Alto Networks, Inc.

전용 로그 수집기에 대한 디바이스 인증서 설치

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• NGFW (Managed by Panorama)	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스 ❑ 아웃바운드 인터넷 액세스 ❑ 다음 사용자 역할 중 하나를 가진 고객 지원 포털(CSP) 계정: 수퍼유저, 표준 사용자, 제한된 사용자, 위협 연구원, AutoFocus 평가판 역할, 그룹 수퍼유저, 그룹 표준 사용자, 그룹 제한된 사용자, 그룹 위협 연구원, 승인된 지원 센터(ASC) 사용자 및 ASC 전체 서비스 사용자 ❑ Panorama 수퍼유저 역할

디바이스 원격 측정을 사용하려면 전용 로그 수집기에 디바이스 인증서를 설치해야 합니다. 디바이스 인증서는 한 번만 설치하면 됩니다. 디바이스 인증서의 수명은 90일입니다. 전용 로그 수집기는 인증서가 만료되기 15일 전에 디바이스 인증서를 다시 설치합니다. 전용 로그 수집기가 자체적으로 디바이스 인증서를 다시 설치할 수 없는 경우 수동으로 만료된 디바이스 인증서를 복원해야 할 수도 있습니다.

디바이스 인증서를 성공적으로 설치하려면 전용 로그 수집기에 아웃바운드 인터넷 연결이 있어야 하며 네트워크에서 다음 정규화된 도메인 이름(FQDN) 및 포트를 허용해야 합니다.

전용 로그 수집기마다 개별적으로 디바이스 인증서를 수동으로 설치해야 합니다. Panorama™ 관리 서버에서 디바이스 인증서를 설치하는 것은 지원되지 않습니다.

FQDN	포트
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 및 TCP 443

©2024 Palo Alto Networks, Inc.

M-300 및 *M-700* 어플라이언스는 초기 등록 프로세스 중 *Palo Alto Networks CSP*에 처음 연결할 때 디바이스 인증서를 자동으로 설치합니다. 이러한 *M-Series* 어플라이언스의 경우 디바이스 인증서를 수동으로 설치할 필요가 없습니다.

STEP 1 | 수퍼유저로 전용 로그 수집기 CLI에 로그인합니다.

Panorama에 디바이스 인증서를 설치하는 데 사용되는 OTP를 적용하려면 수퍼유저 액세스 권한이 있는 관리자가 필요합니다.

STEP 2 | 전용 로그 수집기에서 현재 디바이스 인증서 상태를 확인합니다.

```
admin>show device-certificate status
```

전용 로그 수집기에서 다음 응답 중 하나를 표시합니다.

- 디바이스 인증서가 설치되지 않은 경우 — #### #### ## # ##
- 디바이스 인증서가 만료된 경우 — ## #### ### ##: ###

  응답에는 이전 디바이스 인증서의 수명 및 디바이스 인증서를 마지막으로 가져오려고 시도한 날짜와 시간도 표시됩니다.
- 디바이스 인증서 가져오기에 실패한 경우 — 디바이스 인증서를 마지막으로 가져오려고 시도한 시간이 응답에 표시됩니다.

STEP 3 | 일회용 암호(OTP)를 생성합니다.

OTP 수명은 *60*분이며 *60*분 수명 내에 사용하지 않으면 만료됩니다.

전용 로그 수집기는 *CSP*에서 *OTP* 검색을 한 번만 시도할 수 있습니다. 어떤 이유로든 전용 로그 수집기가 *OTP*를 가져오는 데 실패하면 *OTP*가 만료되며 새 *OTP*를 생성해야 합니다.

1. OTP 생성 권한이 있는 사용자 역할로 고객 지원 포털에 로그인합니다.
2. 제품 > 디바이스 인증서를 선택하고 **OTP** 생성을 선택합니다.
3. 디바이스 유형에서 **Panorama** 관리형 방화벽용 **OTP** 생성을 선택하고 다음을 클릭합니다.
4. **Panorama** 디바이스 일련번호를 선택하고 **OTP** 생성을 선택합니다.
5. **OTP**를 생성하고 OTP를 복사합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | NTP(네트워크 시간 프로토콜) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. 수퍼유저로 전용 로그 수집기 CLI에 로그인합니다.

   Panorama에 디바이스 인증서를 설치하는 데 사용되는 OTP를 적용하려면 수퍼유저 액세스 권한이 있는 관리자가 필요합니다.

2. NTP 서버를 구성합니다.

```
admin>configure
```

```
admin#set deviceconfig system ntp-servers primary-ntp-server
 ntp-server-address <ip_address>
```

```
admin#set deviceconfig system ntp-servers secondary-ntp-server
 ntp-server-address <ip_address>
```

```
admin>commit
```

```
admin>exit
```

STEP 5 | 디바이스 인증서를 설치합니다.

```
admin>request certificate fetch otp <otp_value>
```

STEP 6 | 디바이스 인증서가 성공적으로 설치되었는지 확인합니다.

```
admin> show device-certificate status
```

디바이스 인증서가 성공적으로 설치되면 다음과 같은 응답이 표시됩니다.

```
#### ### ##: ## #### ### ##: ### ## #### #### ##: 2022/11/30 15:17:47
 PST ## #### #### ##: 2023/02/28 15:17:47 PST ##### ### #####:
 2022/11/30 15:29:42 PST ##### ### ##: ## ##### ### ##: #### #### ##### #
##
```


©2024 Palo Alto Networks, Inc.

다른 Panorama 모델로 전환

네트워크 요구 사항이 변경되면(예: 로깅 속도 증가) 이러한 요구 사항을 더 잘 지원하도록 Panorama 관리 서버 및 전용 로그 수집기를 Panorama 모델(으)로 마이그레이션할 수 있습니다.

다른 *Panorama* 모델로 전환하려면 이전 *Panorama*에서 새 *Panorama*로 *Panorama* 구성을 가져와야 합니다. 전환을 시작하기 전에 이전 *Panorama*와 새 *Panorama*가 동일한 *Panorama* 모드(관리 전용 또는 *Panorama* 모드)인지 확인합니다. *Panorama* 모드에 대한 자세한 내용은 Panorama 모델에서 확인할 수 있습니다.

이는 *Panorama* 구성을 새 *Panorama*로 성공적으로 가져오기 위해 필요합니다. *Panorama* 모드 변경에 대한 자세한 내용은 M-시리즈 설정 개요 *M* 시리즈 어플라이언스 및 Panorama 가상 어플라이언스 설정 *Panorama* 가상 어플라이언스를 참조하십시오.

- Panorama 가상 어플라이언스에서 M 시리즈 어플라이언스로 마이그레이션
- Panorama 가상 어플라이언스를 다른 하이퍼바이저로 마이그레이션
- M 시리즈 어플라이언스에서 Panorama 가상 어플라이언스로 마이그레이션
- M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션
- M-100 또는 M-500 어플라이언스에서 M-200 또는 M-600 어플라이언스로 마이그레이션

Panorama 가상 어플라이언스에서 M 시리즈 어플라이언스로 마이그레이션

Panorama 모드에서 Panorama 구성을 Panorama 가상 어플라이언스에서 M-시리즈 어플라이언스로 마이그레이션할 수 있습니다. 그러나 Panorama 가상 어플라이언스의 로그 형식이 M-Series 어플라이언스의 로그 형식과 호환되지 않기 때문에 로그를 마이그레이션할 수 없습니다. 따라서 Panorama 가상 어플라이언스에 저장된 이전 로그에 대한 액세스를 유지하려면 마이그레이션 후 Panorama 가상 어플라이언스를 계속 실행해야 합니다. M-시리즈 어플라이언스는 마이그레이션 후 방화벽이 포워딩하는 새 로그를 수집합니다. 마이그레이션 전 로그가 만료되거나 노후화로 인해 관련이 없는 경우 Panorama 가상 어플라이언스를 종료할 수 있습니다.

레거시 모드는 PAN-OS 8.1 이상의 버전에서 더 이상 지원되지 않습니다. 이전 Panorama 가상 어플라이언스가 레거시 모드에 있는 경우 로그 설정 및 Log Collector 포워딩 구성을 유지하려면 새 하이퍼바이저로 마이그레이션하기 전에 Panorama를 Panorama 모드로 변경해야 합니다. 레거시 모드의 이전 Panorama 구성을 Panorama 모드의 새 Panorama로 가져오면 모든 로그 및 로그 포워딩 설정이 제거됩니다.

하이퍼바이저 간에 로그를 마이그레이션할 수 없습니다. 따라서 이전 Panorama 가상 어플라이언스에 저장된 로그에 대한 액세스를 유지하려면 마이그레이션 후 이전 Panorama 가상 어플라이언스를 계속 실행하고 새 Panorama 가상 어플라이언스에서 관리되는 Log Collector로 추가해야 합니다. 이를 통해 새 Panorama 가상 어플라이언스는 이전 로그 데이터에 대한 액세스를 유지하면서 마이그레이션 후 방화벽이 포워딩하는 새 로그를 수집할 수 있습니다. 마이그레이션 전 로그가 만료되거나 노후화로 인해 관련이 없는 경우 Panorama 가상 어플라이언스를 종료할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스 대신 전용 로그 수집기(로그 수집기 모드의 *M*-시리즈 장비)에 방화벽 로그를 저장하는 경우 전용 로그 수집기를 *Panorama* 모드의 *M*-시리즈 장비로 마이그레이션하여 로그에 대한 액세스를 유지할 수 있습니다.

다른 *Panorama* 모델로 전환할 때 정책 규칙 사용 데이터는 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어, ## 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

STEP 1 | 마이그레이션을 계획합니다.

- M-Series 어플라이언스에 최신 소프트웨어 버전가 필요한 경우 마이그레이션 전에 Panorama 가상 어플라이언스의 소프트웨어를 업그레이드하십시오(M-500 어플라이언스에는 Panorama 7.0 이상의 버전이 필요합니다. M-600 및 M-200 어플라이언스에는 Panorama 8.1 이상의 버전이 필요합니다. M-700 및 M-300 어플라이언스에는 Panorama 11.1 이상 릴리즈가 필요합니다.) 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- 마이그레이션에 대한 유지 관리 기간을 예약합니다. 방화벽은 Panorama 가상 어플라이언스가 오프라인 상태가 된 후 로그를 버퍼링하고 M-시리즈 어플라이언스가 온라인 상태가 된 후 로그를 포워딩할 수 있지만 유지 관리 기간 동안 마이그레이션을 완료하면 로그가 버퍼 용량을 초과하고 Panorama 모델 간의 전환 중에 손실됩니다.
- 기존 로그에 액세스하기 위해 마이그레이션 후 Panorama 가상 어플라이언스에 대한 액세스를 유지할지의 여부를 고려하십시오. 가장 효율적인 접근 방식은 Panorama 가상 어플라이언스에 새 IP 주소를 할당하고 M-시리즈 어플라이언스에 대해 이전 IP 주소를 재사용하는 것입니다. 이렇게 하면 Panorama 가상 어플라이언스에 계속 액세스할 수 있고 각 방화벽에서 Panorama IP 주소를 재구성하지 않고도 방화벽이 M-시리즈 어플라이언스를 가리킬 수 있습니다.

STEP 2 | 새 M-시리즈 어플라이언스를 구입하고 구독을 새 어플라이언스로 마이그레이션하십시오.

1. 새로운 M 시리즈 어플라이언스를 구입합니다.
2. 새로운 지원 라이선스와 마이그레이션 라이선스를 구매하세요.
3. 새 M 시리즈 어플라이언스를 구입할 때 판매 담당자에게 단계적으로 중단하려는 Panorama 가상 어플라이언스의 일련번호 및 디바이스 관리 인증 코드와 선택한 라이선스 마이그레이션 날짜를 제공합니다. M-시리즈 어플라이언스를 받으면 어플라이언스를 등록하고 Palo Alto Networks에서 제공하는 마이그레이션 및 지원 인증 코드를 사용하여 어플라이언스 관리 및 지원 라이선스를 활성화하십시오. 마이그레이션 날짜에 Panorama 가상 어플라이언스의 디바이스 관리 라이선스가 해제되며 더 이상 Panorama 가상 어플라이언스를 사용하여 디바이스를 관리하거나 로그를 수집할 수 없습니다. 그러나 지원 라이선스는 유지되고 Panorama 어플라이언스는 계속 지원됩니다. 유효 날짜 이후에 마이그레이션을 완료할 수 있지만 현재 사용 중지된 Panorama 가상 어플라이언스에서 구성 변경을 커밋할 수 없습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | (레거시 모드만 해당) 이전 Panorama 가상 어플라이언스에서 Panorama 모드로 변경합니다.

> 이 단계는 *Panorama* 가상 어플라이언스의 로그 데이터, 설정 및 로그 포워딩 구성을 유지하는 데 필요합니다. 레거시 모드에서 *Panorama* 구성을 내보내면 이러한 설정이 손실됩니다. 계속하기 전에 *Panorama*를 *Panorama* 모드로 변경하지 않으면 9단계를 완료해야 합니다.
>
> *Panorama* 가상 어플라이언스가 이미 *Panorama* 또는 *Management Only* 모드에 있는 경우 다음 단계를 계속합니다.

STEP 4 | Panorama 가상 어플라이언스에서 Panorama 구성을 내보냅니다.

1. Panorama 가상 어플라이언스에 로그인하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 이름이 지정된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.

STEP 5 | 마이그레이션 후 Panorama 가상 어플라이언스에 액세스할 필요가 없으면 전원을 끄거나 액세스해야 하는 경우 관리(MGT) 인터페이스에 새 IP 주소를 할당하십시오.

Panorama 가상 어플라이언스의 전원을 끄려면 VMware 제품 설명서를 참조하십시오.

Panorama 가상 어플라이언스의 IP 주소를 변경하려면:

1. **Panorama** > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 편집합니다.
2. 새 **IP** 주소를 입력하고 확인을 클릭합니다.
3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 6 | M-시리즈 어플라이언스의 초기 설정을 수행합니다.

1. M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 안내서를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성을 수행하여 라이선스를 활성화하고 업데이트를 설치하는 데 필요한 네트워크 연결을 정의합니다.
3. Panorama를 등록합니다.
4. Panorama 지원 라이선스 활성화.
5. M 시리즈 어플라이언스에서 방화벽 관리 라이선스 활성화/검색. 마이그레이션 라이선스와 연결된 인증 코드를 사용합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. Panorama 가상 어플라이언스와 동일한 버전을 설치합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 가상 어플라이언스에서 M-시리즈 어플라이언스로 내보낸 Panorama 구성 스냅샷을 로드합니다.



새 *Panorama*에서 불러온 *Panorama* 구성을 커밋한 날짜를 반영하도록 *Panorama* 정책 규칙 생성 및 수정 날짜가 업데이트됩니다. 각 정책 규칙의 UUID(Universally Unique Identifier)는 *Panorama* 구성을 마이그레이션할 때 유지됩니다.

관리 방화벽에 대한 생성 및 수정은 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 영향을 받지 않습니다. 이 데이터는 *Panorama*가 아닌 관리 방화벽에 로컬로 저장되기 때문입니다.

1. M 시리즈 어플라이언스에서 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 Panorama 가상 어플라이언스에서 내보낸 Panorama 구성 파일을 찾은 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키(Panorama의 마스터 키)를 선택한 다음 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다.
4. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

STEP 8 | M-시리즈 어플라이언스에서 구성을 수정합니다.

M-시리즈 어플라이언스가 Panorama 가상 어플라이언스와 다른 값을 사용하는 경우 필요합니다. Panorama 가상 어플라이언스에 대한 액세스를 유지하여 해당 로그에 액세스하려면 M-시리즈 어플라이언스에 대해 다른 호스트 이름과 IP 주소를 사용하십시오.

1. **Panorama** > 설정 > 관리를 선택합니다.
2. 일반 설정을 편집하고 호스트 이름을 수정한 다음 확인을 클릭합니다.
3. 관리 인터페이스 설정을 편집하고 필요에 따라 값을 수정한 다음 확인을 클릭합니다.

STEP 9 | 기본 관리형 수집기 및 수집기 그룹을 M 시리즈 어플라이언스에 다시 추가합니다.

Panorama 가상 어플라이언스에서 구성을 로드하면(7단계) 각 M-시리즈 어플라이언스에 사전 정의된 기본 관리형 수집기 및 수집기 그룹이 제거됩니다.

1. M 시리즈 어플라이언스에 로컬인 관리형 수집기를 구성합니다.
2. 기본 관리형 수집기에 대한 수집기 그룹을 구성합니다.
3. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 10 | 디바이스 등록 인증 키를 사용하여 추가된 관리형 방화벽과 전용 로그 수집기에 대한 Panorama에 대한 관리 디바이스 연결 복구를 수행합니다.



이는 한 *Panorama* 모델에서 다른 모델로 전환할 때 필요합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | M-시리즈 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. M 시리즈 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

다른 *Panorama* 모델로 마이그레이션한 후 *Panorama*와 관리형 방화벽 간에 연결 문제가 발생한 경우 Panorama에 대한 관리되는 디바이스 연결을 복구하여 문제를 해결하십시오.

Panorama 가상 어플라이언스를 다른 하이퍼바이저로 마이그레이션

관리 전용 모드 또는 Panorama 모드에서 Panorama 가상 어플라이언스의 Panorama 구성을 지원되는 하나의 하이퍼바이저에서 지원되는 다른 하이퍼바이저로 마이그레이션합니다. Panorama 가상 어플라이언스를 새 하이퍼바이저로 마이그레이션하기 전에 Panorama 모델을(를) 검토하여 마이그레이션하려는 새 하이퍼바이저가 지원되는지 확인합니다. 또한 Panorama 구성에 디바이스 관리를 위한 여러 인터페이스 구성이 있는 경우 디바이스 관리, 로그 수집, 수집기 그룹 통신, 라이선스 및 소프트웨어 업데이트를 위한 여러 인터페이스가 포함된 경우 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 검토하여 마이그레이션하려는 하이퍼바이저가 여러 인터페이스를 지원하는지 확인합니다.

레거시 모드는 PAN-OS 8.1 이상의 버전에서 더 이상 지원되지 않습니다. 이전 Panorama 가상 어플라이언스가 레거시 모드에 있는 경우 로그 설정 및 Log Collector 포워딩 구성을 유지하려면 새 하이퍼바이저로 마이그레이션하기 전에 Panorama를 Panorama 모드로 변경해야 합니다. 레거시 모드의 이전 Panorama 구성을 Panorama 모드의 새 Panorama로 가져오면 모든 로그 및 로그 포워딩 설정이 제거됩니다.

Panorama 가상 어플라이언스에서 로그를 마이그레이션할 수 없습니다. 따라서 이전 Panorama 가상 어플라이언스에 저장된 로그에 대한 액세스를 유지하려면 마이그레이션 후 Log Collector 모드에서 이전 Panorama 가상 어플라이언스를 계속 실행하고 새 Panorama 가상 어플라이언스에서 관리되는 Log Collector로 추가해야 합니다. 이를 통해 새 Panorama 가상 어플라이언스는 이전 로그 데이터에 대한 액세스를 유지하면서 마이그레이션 후 방화벽이 포워딩하는 새 로그를 수집할 수 있습니다. 마이그레이션 전 로그가 만료되거나 노후화로 인해 관련이 없는 경우 Panorama 가상 어플라이언스를 종료할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 가상 어플라이언스 대신 전용 로그 수집기(로그 수집기 모드의 *Panorama* 가상 어플라이언스)에 방화벽 로그를 저장하는 경우 전용 로그 수집기를 *Panorama* 모드의 새 *Panorama* 가상 어플라이언스로 마이그레이션하여 로그에 대한 액세스를 유지할 수 있습니다.

다른 *Panorama* 모델로 전환할 때 정책 규칙 사용 데이터는 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어, ## 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

STEP 1 | 마이그레이션을 계획합니다.

- 새 Panorama 가상 어플라이언스에 현재 소프트웨어의 최신 버전가 필요한 경우 마이그레이션 전에 Panorama 가상 어플라이언스의 소프트웨어를 업그레이드하십시오. 각 하이퍼바이저의 최소 PAN-OS 버전은 Panorama Hypervisor 지원을 참조하십시오. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- 마이그레이션에 대한 유지 관리 기간을 예약합니다. 방화벽은 Panorama 가상 어플라이언스가 오프라인 상태가 된 후 로그를 버퍼링하고 새 Panorama 가상 어플라이언스가 온라인 상태가 된 후 로그를 포워딩할 수 있지만 유지 관리 기간 동안 마이그레이션을 완료하면 로그가 버퍼 용량을 초과하고 하이퍼바이저 간의 전환 중에 손실됩니다.
- 기존 로그에 액세스하기 위해 마이그레이션한 후 이전 Panorama 가상 어플라이언스에 대한 액세스를 유지할지의 여부를 고려하십시오. 가장 효율적인 접근 방식은 기존 Panorama 가상 어플라이언스에 새 IP 주소를 할당하고 Panorama 가상 어플라이언스에 대해 기존 IP 주소를 재사용하는 것입니다. 이렇게 하면 각 방화벽에서 Panorama IP 주소를 재구성하지 않고도 기존 Panorama 가상 어플라이언스에 계속 액세스할 수 있고 방화벽이 새 Panorama 가상 어플라이언스를 가리킬 수 있습니다.

  이전 Panorama 가상 어플라이언스에 대한 액세스를 유지하려면 마이그레이션을 성공적으로 완료하기 전에 새 Panorama 가상 어플라이언스에 대한 새 디바이스 관리 라이선스 및 지원 라이선스를 구매해야 합니다.

STEP 2 | (레거시 모드만 해당) 이전 Panorama 가상 어플라이언스에서 Panorama 모드에서 Panorama 가상 어플라이언스 설정.

이 단계는 이전 *Panorama* 가상 어플라이언스의 로그 설정(***Panorama*** > 로그 설정)을 유지하는 데 필요합니다. 레거시 모드에서 *Panorama* 구성을 내보내면 이러한 설정이 손실됩니다.

Panorama 가상 어플라이언스가 이미 *Panorama* 또는 *Management Only* 모드에 있는 경우 다음 단계를 계속합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 이전 Panorama 가상 어플라이언스에서 Panorama 구성을 내보냅니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 `running-config.xml`을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.
4. 내보낸 `running-config.xml` 파일을 찾아 XML 파일의 이름을 바꿉니다. Panorama는 이름이 `running-config.xml`인 XML 파일 가져오기를 지원하지 않으므로 구성을 가져오는 데 필요합니다.

STEP 4 | 파노라마 가상 어플라이언스를 설치합니다.

STEP 5 | 이전 Panorama 가상 어플라이언스의 일련 번호를 새 Panorama 가상 어플라이언스로 마이그레이션합니다.

이 단계는 *Panorama* 일련번호에 연결된 모든 구독 및 디바이스 관리 라이선스를 마이그레이션하는 데 필요하며 이전 *Panorama* 가상 어플라이언스를 종료하려는 경우에만 필요합니다. 이전 *Panorama* 가상 어플라이언스에 대한 액세스를 유지하려는 경우 다음 단계를 계속하십시오.

이전 *Panorama* 가상 어플라이언스를 종료할 수 있는 기간은 최대 *90*일입니다. 동일한 일련번호로 여러 *Panorama* 가상 어플라이언스를 실행하면 *EULA*를 위반합니다.

1. 이전 Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인합니다.
2. 대시보드에서 일반 정보 위젯에 있는 이전 Panorama 가상 어플라이언스의 ####를 복사합니다.
3. 새 Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인합니다.
4. 새 Panorama 가상 어플라이언스에 이전 Panorama 가상 어플라이언스의 일련번호를 추가합니다.
   1. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
   2. 일련번호를 입력(붙여넣기)하고 확인을 클릭합니다.
   3. 커밋 및 **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 새 Panorama 가상 어플라이언스의 초기 설정을 수행합니다.

1. 라이선스를 활성화하고 업데이트를 설치하는 데 필요한 네트워크 연결을 정의하려면 Panorama 가상 어플라이언스의 초기 구성 수행을(를) 수행합니다.
2. (이전 Panorama 가상 어플라이언스에 대한 액세스를 유지하는 경우에만) Panorama를 등록합니다.
3. (이전 Panorama 가상 어플라이언스에 대한 액세스를 유지하는 경우에만) Panorama 지원 라이선스를 활성화합니다.
4. (이전 Panorama 가상 어플라이언스에 대한 액세스를 유지하는 경우에만) Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색. 마이그레이션 라이선스와 연결된 인증 코드를 사용합니다.
5. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. 이전 Panorama 가상 어플라이언스와 동일한 버전을 설치합니다.

   이 단계는 이전 *Panorama* 가상 어플라이언스에서 구성을 로드하기 전에 필요합니다. 보안 중단을 방지하기 위해 필요한 모든 콘텐츠 업데이트가 설치되어 있는지 확인합니다.
6. **Panorama** > 플러그인을 선택한 다음 이전 Panorama 가상 어플라이언스에 설치된 모든 플러그인을 설치합니다.

STEP 7 | 마이그레이션 후 액세스할 필요가 없는 경우 이전 Panorama 가상 어플라이언스의 전원을 끄거나 액세스해야 하는 경우 관리(MGT) 인터페이스에 새 IP 주소를 할당하십시오.

Panorama 가상 어플라이언스의 전원을 끄려면 이전 Panorama 가상 어플라이언스가 배포된 하이퍼바이저에 대해 지원되는 설명서를 참조하십시오.

Panorama 가상 어플라이언스의 IP 주소를 변경하려면:

1. 이전 Panorama 가상 어플라이언스의 웹 인터페이스에서 **Panorama** > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 편집합니다.
2. 새 **IP** 주소를 입력하고 확인을 클릭합니다.
3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 8 | (Prisma Access) 기존 Panorama 가상 어플라이언스에서 새 Panorama 가상 어플라이언스로 Prisma Access 라이선스를 이전합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 이전 Panorama 가상 어플라이언스에서 새 Panorama 가상 어플라이언스로 내보낸 Panorama 구성 스냅샷을 로드합니다.

> 새 *Panorama*에서 불러온 *Panorama* 구성을 커밋한 날짜를 반영하도록 *Panorama* 정책 규칙 생성 및 수정 날짜가 업데이트됩니다. 각 정책 규칙의 UUID(Universally Unique Identifier)는 *Panorama* 구성을 마이그레이션할 때 유지됩니다.
>
> 관리 방화벽에 대한 생성 및 수정은 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 영향을 받지 않습니다. 이 데이터는 *Panorama*가 아닌 관리 방화벽에 로컬로 저장되기 때문입니다.

1. 새로운 Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 Panorama 가상 어플라이언스에서 내보낸 Panorama 구성 파일을 찾은 다음 확인을 클릭합니다.
4. 이름이 지정된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키를 공백(비어 있음)으로 두고 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다.
5. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

STEP 10 | 새 Panorama 가상 어플라이언스에서 구성을 수정합니다.

새 Panorama 가상 어플라이언스가 이전 Panorama 가상 어플라이언스와 다른 값을 사용하는 경우 필요합니다. 기존 Panorama 가상 어플라이언스에 대한 액세스를 유지하여 해당 로그에 액세스하려면 새 Panorama 가상 어플라이언스에 대해 다른 호스트 이름과 IP 주소를 사용하십시오.

1. **Panorama** > 설정 > 관리를 선택합니다.
2. 일반 설정을 편집하고 호스트 이름을 수정한 다음 확인을 클릭합니다.
3. 관리 인터페이스 설정을 편집하고 필요에 따라 값을 수정한 다음 확인을 클릭합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 11 | 새 Panorama 가상 어플라이언스에 기본 관리형 수집기 및 수집기 그룹을 추가합니다.

이전 Panorama 가상 어플라이언스에서 구성을 로드하면(7단계) Panorama 모드의 각 Panorama 가상 어플라이언스에 사전 정의된 기본 관리형 수집기 및 수집기 그룹이 제거됩니다.

1. 이전 Panorama 가상 어플라이언스에 저장된 로그에 대한 액세스를 유지하려면 Log Collector 모드로 변경하고 전용 로그 수집기를 새 Panorama 가상 어플라이언스에 추가하십시오.
   1. Panorama 가상 어플라이언스를 로그 수집기로 설정.
   2. 관리형 수집기 구성.
2. Panorama 가상 어플라이언스에 로컬인 관리형 수집기를 구성합니다.
3. 기본 관리형 수집기에 대한 수집기 그룹을 구성합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

©2024 Palo Alto Networks, Inc.

STEP 12 | 디바이스 등록 인증 키를 사용하여 추가된 관리형 방화벽과 전용 로그 수집기에 대한 Panorama에 대한 관리 디바이스 연결 복구를 수행합니다.

이는 한 *Panorama* 모델에서 다른 모델로 전환할 때 필요합니다.

STEP 13 | 새로운 Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개하십시오.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. 새 Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

다른 *Panorama* 모델로 마이그레이션한 후 *Panorama*와 관리형 방화벽 간에 연결 문제가 발생한 경우 Panorama에 대한 관리되는 디바이스 연결을 복구하여 문제를 해결하십시오.

M 시리즈 어플라이언스에서 Panorama 가상 어플라이언스로 마이그레이션

파노라마 모드의 파노라마 구성을 M-100, M-200, M-300, M-500, M-600, M-700 어플라이언스에서 Panorama 가상 어플라이언스로 마이그레이션할 수 있습니다. 그러나 M-Series 어플라이언스의 로그 형식이 Panorama 가상 어플라이언스의 로그 형식과 호환되지 않기 때문에 로그를 마이그레이션할 수 없습니다. 따라서 M-Series 어플라이언스에 저장된 이전 로그에 대한 액세스를 유지하려면 마이그레이션 후 M-Series 어플라이언스를 전용 로그 수집기로 계속 실행하고 Panorama 가상 어플라이언스에 관리되는 수집기로 추가해야 합니다.

Panorama 관리 서버가 고가용성 구성의 일부인 경우 동일한 하이퍼바이저 또는 클라우드 환경의 두 번째 Panorama 가상 어플라이언스를 배포하고 필요한 디바이스 관리 및 지원 라이선스를 구매해야 합니다. HA 요구 사항의 전체 목록은 Panorama HA 전제 조건을 참조하십시오.

다른 *Panorama* 모델로 전환하면 정책 규칙 사용 데이터가 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어 ## 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 마이그레이션을 계획합니다.

- ❑ Panorama 가상 어플라이언스로 마이그레이션하기 전에 M-Series 어플라이언스를 PAN-OS 11.1 이상의 버전으로 업그레이드합니다. Panorama를 업그레이드하려면 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치를 참조하십시오. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- ❑ 마이그레이션에 대한 유지 관리 기간을 예약합니다. 방화벽은 M-시리즈 어플라이언스가 오프라인 상태가 된 후 로그를 버퍼링한 다음 Panorama 가상 어플라이언스가 온라인 상태가 된 후 로그를 포워딩할 수 있지만 유지 관리 기간 동안 마이그레이션을 완료하면 다른 Panorama 모델로 전환하는 동안 로그가 버퍼 용량을 초과할 위험이 최소화됩니다.

STEP 2 | 새로운 Panorama 가상 어플라이언스에 대한 관리 및 지원 라이선스를 구매하십시오.

1. 새 디바이스 관리 및 지원 라이선스를 구입하려면 영업 담당자에게 문의하십시오.
2. 단계적으로 중단할 M 시리즈 어플라이언스의 일련번호, 새 Panorama 가상 어플라이언스를 구입할 때 받은 일련번호 및 지원 인증 코드, 이전 디바이스에서 새 가상 어플라이언스로 마이그레이션이 완료되는 예상 날짜를 영업 담당자에게 제공합니다. 마이그레이션 날짜 전에 일련번호를 등록하고 마이그레이션을 시작할 수 있도록 새 가상 어플라이언스에서 지원 인증 코드를 활성화하십시오. 이전 M 시리즈 어플라이언스의 용량 인증 코드는 제공한 예상 마이그레이션 완료 날짜에 자동으로 제거됩니다.

STEP 3 | Panorama 가상 어플라이언스의 초기 설정을 수행합니다.

1. Panorama 가상 어플라이언스 설정.
2. Panorama Virtual Appliance의 초기 구성을 수행하여 라이선스를 활성화하고 업데이트를 설치하는 데 필요한 네트워크 연결을 정의합니다.
3. Panorama를 등록합니다.
4. Panorama 지원 라이선스 활성화.
5. Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스 활성화/검색
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. M 시리즈 어플라이언스와 동일한 버전을 설치합니다.

STEP 4 | 관리 인터페이스만 사용하도록 M-시리즈 어플라이언스 Panorama 인터페이스 구성을 편집합니다.

Panorama 가상 어플라이언스는 디바이스 관리 및 로그 수집을 위한 관리 인터페이스만 지원합니다.

1. M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택합니다.
3. 일반 설정을 편집하고 호스트 이름을 수정한 다음 확인을 클릭합니다.
4. 인터페이스를 선택한 다음 관리 인터페이스를 편집하여 필요한 서비스를 활성화합니다.
5. 나머지 인터페이스에 대한 서비스를 비활성화합니다.
6. 커밋 > **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 새 Panorama 가상 어플라이언스의 IP 주소를 추가합니다.

M 시리즈 어플라이언스에서 Panorama 가상 어플라이언스의 공용 IP 주소를 두 번째 Panorama Server로 추가하여 새 Panorama 관리 서버에서 디바이스를 관리합니다. Panorama 가상 어플라이언스가 Alibaba Cloud, AWS, Azure, GCP 또는 OCI에 배포된 경우 공용 IP 주소를 사용합니다.

1. 디바이스 > 설정을 선택합니다.
2. 템플릿 컨텍스트 드롭다운에서 Panorama 서버 구성이 포함된 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
3. Panorama 설정을 편집합니다.
4. Panorama 가상 어플라이언스 공용 IP 주소를 입력하고 확인을 클릭합니다.
5. 커밋 > 커밋 및 푸시를 선택합니다.

STEP 6 | M-시리즈 어플라이언스에서 구성을 내보냅니다.

1. **Panorama** > 설정 > 작업을 선택합니다.
2. 이름이 지정된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다. Panorama 어플라이언스 외부의 위치에 구성을 저장합니다.

STEP 7 | M-시리즈 어플라이언스의 전원을 끄거나 관리(MGT) 인터페이스에 새 IP 주소를 할당합니다.

*M-*시리즈 어플라이언스가 *Panorama* 모드이고 새 *Panorama* 가상 어플라이언스에 액세스해야 하는 로컬 *Log Collector*에 로그가 저장된 경우 *M-*시리즈 어플라이언스를 관리되는 로그 수집기로써 *Panorama* 가상 어플라이언스에 추가하려면 *IP* 주소를 변경해야 합니다.

- **M-**시리즈 어플라이언스의 전원을 끄려면**:**

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > **Setup** > **Operations**를 선택한 다음 Device Operations에서 **Shutdown Panorama**를 선택합니다. 예를 클릭하여 종료를 확인합니다.

- **M-**시리즈 어플라이언스에서 **IP** 주소를 변경하려면**:**

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > **Setup** > **Management**를 선택한 다음 관리 인터페이스 설정을 편집합니다.
3. 새 **IP** 주소를 입력하고 확인을 클릭합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | M-시리즈 어플라이언스에서 Panorama 가상 어플라이언스로 내보낸 Panorama 구성 스냅샷을 로드합니다.



새 *Panorama*에서 불러온 *Panorama* 구성을 커밋한 날짜를 반영하도록 *Panorama* 정책 규칙 생성 및 수정 날짜가 업데이트됩니다. 각 정책 규칙의 UUID(Universally Unique Identifier)는 *Panorama* 구성을 마이그레이션할 때 유지됩니다.

관리 방화벽에 대한 생성 및 수정은 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 영향을 받지 않습니다. 이 데이터는 *Panorama*가 아닌 관리 방화벽에 로컬로 저장되기 때문입니다.

1. Panorama 가상 어플라이언스의 Panorama 웹 인터페이스에 로그인하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 M 시리즈 어플라이언스에서 내보낸 Panorama 구성 파일을 찾은 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키(Panorama의 마스터 키)를 선택한 다음 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다.

오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오. 커밋이 성공하면 구성이 로드됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 기존 로그 데이터를 보존하려면 M-Series 어플라이언스를 Log Collector 모드로 변경하십시오.

로깅 디스크가 *M-Series* 어플라이언스에 여전히 삽입되어 있는 동안 *Log Collector* 모드로 변경하면 로깅 데이터가 지워집니다. 로그 데이터 손실을 방지하려면 모드를 변경하기 전에 로깅 디스크를 제거해야 합니다.

각 디스크 쌍에 대한 메타데이터를 생성하면 인덱스가 다시 작성됩니다. 따라서 데이터 크기에 따라 이 프로세스를 완료하는 데 시간이 오래 걸릴 수 있습니다. 프로세스를 가속화하기 위해 여러 *CLI* 세션을 시작하고 각 세션에서 메타데이터 재생성 명령을 실행하여 모든 쌍에 대해 동시에 프로세스를 완료할 수 있습니다. 자세한 내용은 M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성을 참조하십시오.

1. 이전 M-시리즈 어플라이언스에서 RAID 디스크를 제거합니다.
   1. 시스템이 종료될 때까지 전원 버튼을 눌러 M-시리즈 어플라이언스의 전원을 끕니다.
   2. 디스크 쌍을 제거합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.
2. 전원 버튼을 눌러 M-시리즈 어플라이언스의 전원을 켭니다.
3. ### 수퍼유저 관리자 계정을 구성합니다.

   ### 관리자 계정이 이미 생성된 경우 다음 단계를 계속합니다.

   로그 수집기 모드로 전환하기 전에 운용 관리자 권한이 있는 ### 계정을 생성해야 합니다. 그렇지 않으면 모드 전환 후 *M*-시리즈 어플라이언스에 액세스할 수 없습니다.
4. 이전 M 시리즈 어플라이언스에서 Panorama CLI에 로그인합니다.
5. Panorama 모드에서 로그 수집기 모드로 전환합니다.
   - 다음 명령을 입력하여 로그 수집기 모드로 전환합니다.

     ```
     > request system system-mode logger
     ```
   - **Y**를 입력하여 모드 변경을 확인합니다. M-시리즈 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 M-시리즈 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 확인하십시오.

     CMS ### 프롬프트가 표시되면 로그 수집기가 재부팅을 완료하지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 *Enter* 키를 누릅니다.
   - CLI에 다시 로그인합니다.
   - 로그 수집기 모드로의 전환이 성공했는지 확인합니다.

     ```
     > show system info | match system-mode
     ```

     모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

```
> system-mode: logger
```

6. 디스크를 이전 M 시리즈 어플라이언스에 다시 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

   디스크 쌍 연결을 유지해야 합니다. 슬롯 A1/A2의 디스크 쌍을 슬롯 B1/B2에 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.
7. 각 쌍에 대해 다음 CLI 명령을 실행하여 디스크 쌍을 활성화하십시오.

   ```
   > request system raid add <slot> force no-format
   ```

   예:

   ```
   > request system raid add A1 force no-format > request system
    raid add A2 force no-format
   ```

   force 및 **no-format** 인수가 필요합니다. **force** 인수는 디스크 쌍을 새 어플라이언스와 연결합니다. **no-format** 인수는 드라이브의 재포맷을 방지하고 디스크에 저장된 로그를 유지합니다.
8. 각 디스크 쌍에 대한 메타데이터를 생성합니다.

   ```
   > request metadata-regenerate slot <slot_number>
   ```

   예:

   ```
   > request metadata-regenerate slot 1
   ```
9. Log Collector와 Panorama 관리 서버 간의 연결을 활성화합니다.

   로그 수집기 CLI에서 다음 명령을 입력합니다. 여기서 *<IPaddress1>*은(는) 단독(비HA) 또는 활성(HA) Panorama의 MGT 인터페이스용이고 *<IPaddress2>*은(는) 패시브(HA) Panorama의 MGT 인터페이스용입니다.

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress1> panorama-server-2 <IPaddress2> # commit
    # exit
   ```

STEP 10 | 디바이스 등록 인증 키를 사용하여 추가된 관리형 방화벽과 전용 로그 수집기에 대한 Panorama에 대한 관리 디바이스 연결 복구를 수행합니다.

이는 한 *Panorama* 모델에서 다른 모델로 전환할 때 필요합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | Panorama 가상 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. Panorama 가상 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽이 연결됨으로 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹을 선택한 다음 디바이스 및 네트워크 템플릿 포함을 선택합니다.
   3. 수집기 그룹을 선택한 다음 모든 수집기 그룹을 선택한 다음 확인을 클릭합니다.
   4. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

STEP 12 | (HA만 해당) Panorama HA 피어를 설정합니다.

Panorama 관리 서버가 고가용성 구성에 있는 경우 HA 피어에서 아래 단계를 수행합니다.

1. Panorama 가상 어플라이언스의 초기 설정을 수행합니다.
2. 관리 인터페이스만 사용하도록 M-시리즈 어플라이언스 Panorama 인터페이스 구성을 편집합니다.
3. 새 Panorama 가상 어플라이언스의 IP 주소를 추가합니다.
4. M-시리즈 어플라이언스의 전원을 끄거나 관리(MGT) 인터페이스에 새 IP 주소를 할당합니다.
5. 기존 로그 데이터를 보존하려면 M-Series 어플라이언스를 Log Collector 모드로 변경하십시오.

STEP 13 | (HA만 해당) Panorama 가상 어플라이언스 HA 피어 구성을 수정합니다.

1. HA 피어에서 Panorama 웹 인터페이스에 로그인하고 **Panorama** > 고가용성을 선택한 다음 설정을 편집합니다.
2. 피어 **HA IP** 주소 필드에 HA 피어의 새 IP 주소를 입력하고 확인을 클릭합니다.
3. 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.
4. HA 피어의 다른 피어에서 이 단계를 반복합니다.

©2024 Palo Alto Networks, Inc.

STEP 14 | (HA만 해당) Panorama 피어를 동기화합니다.

1. HA 피어 중 하나에서 대시보드에 액세스하고 위젯 > 시스템 > 고가용성을 선택하여 HA 위젯을 표시합니다.
2. 피어에 동기화하고 예를 클릭한 다음 실행 중인 구성이 동기화됨을 표시할 때까지 기다립니다.
3. 나머지 HA 피어에서 대시보드에 액세스하고 위젯 > 시스템 > 고가용성을 선택하여 HA 위젯을 표시합니다.
4. 실행 중인 구성이 동기화됨을 표시하는지 확인합니다.

다른 *Panorama* 모델로 마이그레이션한 후 *Panorama*와 관리형 방화벽 간에 연결 문제가 발생한 경우 Panorama에 대한 관리되는 디바이스 연결을 복구하여 문제를 해결하십시오.

M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션

Panorama 모드(Panorama 관리 서버)에서 Panorama 구성 및 방화벽 로그를 M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션할 수 있습니다. Log Collector 모드(전용 로그 수집기)에서 방화벽 로그를 M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션할 수도 있습니다. 수집기 그룹의 모든 로그 수집기는 동일한 Panorama 모델이어야 하므로 수집기 그룹의 M-100 어플라이언스를 모두 마이그레이션하거나 전혀 마이그레이션하지 않아야 합니다.

다음 절차에서 Panorama 관리 서버는 능동/수동 고가용성(HA) 구성으로 배포되며 구성과 로그를 모두 마이그레이션하고 M-500 어플라이언스는 M-100 어플라이언스의 IP 주소를 재사용합니다.

이 절차에서는 더 이상 디바이스 관리 또는 로그 수집에 *M-100*을 사용하지 않는다고 가정합니다. 폐기된 *M-100* 어플라이언스를 전용 로그 수집기로 사용하려는 경우 *M-100*에 디바이스 관리 라이선스가 필요합니다. 디바이스 관리 라이선스가 없으면 *M-100*을 전용 로그 수집기로 사용할 수 없습니다.

M-100 어플라이언스를 전용 로그 수집기로 사용할 계획이 없지만 *M-100* 어플라이언스에 나중에 액세스해야 하는 로그 데이터가 포함된 경우에도 기존 로그 데이터를 사용하여 보고서를 쿼리하고 생성할 수 있습니다. *Palo Alto Networks*는 *M-100* 어플라이언스를 폐기하기 전에 로그 보존 정책을 검토할 것을 권장합니다.

Panorama 구성이 아닌 로그만 마이그레이션하려는 경우 로그 수집기 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션 또는 Panorama 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션 작업을 수행합니다.

HA 구성에 배포되지 않은 새 *Panorama* 관리 서버로 마이그레이션하고 새 *Panorama*가 기존 전용 로그 수집기의 로그에 액세스해야 하는 경우 비HA Panorama의 실패/RMA 후 로그 수집기 마이그레이션 작업을 수행하십시오.

다른 *Panorama* 모델로 전환할 때 정책 규칙 사용 데이터는 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어, ## 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 마이그레이션을 계획합니다.

- 현재 버전가 7.0 이전인 경우 M-100 어플라이언스의 소프트웨어를 업그레이드하십시오. M-500 어플라이언스에는 Panorama 7.0 이상의 버전이 필요합니다. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- 이러한 로그를 보존하려면 마이그레이션 전에 Panorama 및 Log Collectors가 생성하는 시스템 및 구성 로그를 외부 대상으로 포워딩하십시오. Panorama 모드의 M-시리즈 어플라이언스는 모델 간에 이동할 수 없는 SSD에 이러한 로그 유형을 저장합니다. 방화벽 로그를 저장하는 RAID 드라이브만 이동할 수 있습니다.
- 마이그레이션에 대한 유지 관리 기간을 예약합니다. 방화벽은 M-100 어플라이언스가 오프라인 상태가 된 후 로그를 버퍼링하고 M-500 어플라이언스가 온라인 상태가 된 후 로그를 포워딩할 수 있지만 유지 관리 기간 동안 마이그레이션을 완료하면 로그가 버퍼 용량을 초과하여 Panorama 모델 간의 전환 중에 손실될 위험이 최소화됩니다.

STEP 2 | 새 M-500 어플라이언스를 구입하고 구독을 새 어플라이언스로 마이그레이션하십시오.

1. 새로운 M-500 어플라이언스를 구입합니다.
2. 새로운 지원 라이선스와 마이그레이션 라이선스를 구매하세요.
3. 새 M-500 어플라이언스를 구입할 때 판매 담당자에게 단계적으로 중단하려는 M-100 어플라이언스의 일련번호 및 디바이스 관리 인증 코드와 선택한 라이선스 마이그레이션 날짜를 제공합니다. M-500 어플라이언스를 받으면 어플라이언스를 등록하고 Palo Alto Networks에서 제공하는 마이그레이션 및 지원 인증 코드를 사용하여 어플라이언스 관리 및 지원 라이선스를 활성화하십시오. 마이그레이션 날짜에 M-100의 디바이스 관리 라이선스가 해제되며 더 이상 M-100 어플라이언스를 사용하여 디바이스를 관리하거나 로그를 수집할 수 없습니다. 그러나 지원 라이선스는 유지되고 Panorama 어플라이언스는 계속 지원됩니다. 유효 날짜 이후에 마이그레이션을 완료할 수 있지만 현재 사용 중지된 M-100 어플라이언스에서 구성 변경 사항을 커밋할 수 없습니다.

STEP 3 | Panorama 모드에서 각 M-100 어플라이언스의 Panorama 구성을 내보냅니다.

각 M-100 어플라이언스 HA 피어에서 다음 작업을 수행합니다.

1. M-100 어플라이언스에 로그인하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 이름이 지정된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.

STEP 4 | Panorama 모드에서 각 M-100 어플라이언스의 전원을 끕니다.

1. 전원을 끌 M-100 어플라이언스 HA 피어에 로그인합니다.
2. **Panorama** > 설정 > 작업을 선택한 다음 **Panorama** 종료를 클릭합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 각 M-500 어플라이언스의 초기 설정을 수행합니다.

1. M-500 어플라이언스를 랙에 장착합니다. 지침은 M-500 어플라이언스 하드웨어 참조 안내서를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성을 수행하여 라이선스를 활성화하고 업데이트를 설치하는 데 필요한 네트워크 연결을 정의합니다.
3. Panorama를 등록합니다.
4. Panorama 지원 라이선스 활성화.
5. 방화벽 관리 라이선스를 활성화합니다. 마이그레이션 라이선스와 연결된 인증 코드를 사용합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. M-100 어플라이언스와 동일한 버전을 설치합니다.
7. (전용 로그 수집기만 해당) M 시리즈 어플라이언스를 로그 수집기로 설정합니다.

STEP 6 | 각 M-100 어플라이언스에서 내보낸 Panorama 구성 스냅샷을 Panorama 모드(두 HA 피어 모두)의 각 M-500 어플라이언스로 로드합니다.

새 *Panorama*에서 불러온 *Panorama* 구성을 커밋한 날짜를 반영하도록 *Panorama* 정책 규칙 생성 및 수정 날짜가 업데이트됩니다. 각 정책 규칙의 UUID(Universally Unique Identifier)는 *Panorama* 구성을 마이그레이션할 때 유지됩니다.

관리 방화벽에 대한 생성 및 수정은 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 영향을 받지 않습니다. 이 데이터는 *Panorama*가 아닌 관리 방화벽에 로컬로 저장되기 때문입니다.

각 M-500 어플라이언스 HA 피어에서 다음 작업을 수행합니다.

1. M-500 어플라이언스에 로그인하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 M-500 어플라이언스와 동일한 HA 우선순위(기본 또는 보조)를 갖는 M-100 어플라이언스에서 내보낸 구성 파일을 찾은 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키(Panorama의 마스터 키)를 선택한 다음 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 커밋을 확인합니다. 계속하기 전에 오류를 해결합니다.
5. Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 7 | Panorama 모드에서 M-500 어플라이언스 HA 피어 간의 구성을 동기화합니다.

1. 활성 M-500 어플라이언스에서 대시보드 탭을 선택한 다음 고가용성 위젯에서 피어에 동기화를 클릭합니다.
2. 고가용성 위젯에서 로컬(기본 M-500 어플라이언스)이 활성이고 피어가 수동이며 실행 중인 구성이 동기화되었는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | RAID 드라이브를 각 M-100 어플라이언스에서 교체용 M-500 어플라이언스로 이동하여 방화벽에서 수집된 로그를 마이그레이션합니다.

다음 작업에서 M-500 어플라이언스에서 이미 완료한 모든 단계를 건너뜁니다.

- Panorama 모드에서 새 M-시리즈 어플라이언스로 로그를 마이그레이션합니다. 로그 수집을 위해 기본 관리형 수집기를 사용하는 경우에만 M-100 어플라이언스에서 로그를 마이그레이션하십시오.
- 로그 수집기 모드에서 새 M-시리즈 어플라이언스로 로그를 마이그레이션합니다.

STEP 9 | 디바이스 등록 인증 키를 사용하여 추가된 관리형 방화벽과 전용 로그 수집기에 대한 Panorama에 대한 관리 디바이스 연결 복구를 수행합니다.

이는 한 *Panorama* 모델에서 다른 모델로 전환할 때 필요합니다.

STEP 10 | Panorama 모드에서 활성 M-500 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. 활성 M-500 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 연결됨이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 동기화되지 않음을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 디바이스로 푸시 > 커밋을 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

다른 *Panorama* 모델로 마이그레이션한 후 *Panorama*와 관리형 방화벽 간에 연결 문제가 발생한 경우 Panorama에 대한 관리되는 디바이스 연결을 복구하여 문제를 해결하십시오.

M-100 또는 M-500 어플라이언스에서 M-200 또는 M-600 어플라이언스로 마이그레이션

이 절차에서는 Panorama 모드(Panorama 관리 서버) 에서 다음 M 시리즈 어플라이언스에 대한 Panorama 구성 마이그레이션에 대해 설명합니다.

- M-100 어플라이언스를 M-200 또는 M-600 어플라이언스에 연결합니다.

  로그 마이그레이션은 지원되지 않습니다. M-100 어플라이언스 로깅 디스크 폼 팩터는 M-200 및 M-600 어플라이언스에서 지원되지 않습니다.

 ©2024 Palo Alto Networks, Inc.

- M-500 어플라이언스를 M-200 또는 M-600 어플라이언스에 연결합니다.

  로그 마이그레이션은 지원되지 않습니다. M-500 어플라이언스 로깅 디스크 폼 팩터는 M-200 및 M-600 어플라이언스에서 지원되지 않습니다.

또한 수집기 그룹의 모든 로그 수집기는 동일한 Panorama 모델이어야 합니다. 예를 들어, 새 M-200 어플라이언스의 로컬 로그 수집기를 수집기 그룹에 추가하려면 대상 수집기 그룹에 M-200 어플라이언스만 포함되어야 합니다. M-600 어플라이언스의 로컬 로그 수집기도 마찬가지입니다.

이 절차에서는 디바이스 관리 또는 로그 수집을 위해 더 이상 *M-100* 또는 *M-500* 어플라이언스를 사용하지 않는다고 가정합니다. 폐기된 *M-100* 또는 *M-500* 어플라이언스를 전용 로그 수집기로 사용하려는 경우 *M-100* 또는 *M-500* 어플라이언스에 디바이스 관리 라이선스가 필요합니다. 디바이스 관리 라이선스가 없으면 *M-100* 또는 *M-500*을 전용 로그 수집기로 사용할 수 없습니다.

M-100 또는 *M-500* 어플라이언스를 전용 로그 수집기로 사용하지 않으려는 경우 나중에 기존 로그 데이터에 계속 액세스할 수 있습니다. 새 *M* 시리즈 어플라이언스로 성공적으로 마이그레이션한 후 *M-100* 또는 *M-500* 어플라이언스의 전원을 켜서 해제된 *M* 시리즈 어플라이언스의 Panorama 웹 인터페이스에서 보고서를 쿼리하고 생성합니다. *Palo Alto Networks*는 *M-100* 또는 *M-500* 어플라이언스를 폐기하기 전에 로그 보존 정책을 검토할 것을 권장합니다.

다른 *Panorama* 모델로 전환할 때 정책 규칙 사용 데이터는 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어, *##* 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

STEP 1 | 마이그레이션을 계획합니다.

- M-100 또는 M-500 어플라이언스의 소프트웨어를 지원되는 PAN-OS 릴리스로 업그레이드합니다. Palo Alto 네트워크 호환성 매트릭스에서 지원되는 최소 PAN-OS 버전을 확인합니다.

  현재 지원되는 PAN-OS 버전 목록은 Palo Alto Networks 단종 요약을 참조하십시오. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- 마이그레이션에 대한 유지 관리 기간을 예약합니다. 방화벽은 M-100 또는 M-500 어플라이언스가 오프라인 상태가 된 후 로그를 버퍼링하고 M-200 또는 M-600 어플라이언스가 온라인 상태가 된 후 로그를 포워딩할 수 있지만 유지 관리 기간 동안 마이그레이션을 완료하면 로그가 버퍼 용량을 초과하여 Panorama 모델 간의 전환 중에 손실될 위험이 최소화됩니다.

STEP 2 | 새 M-200 또는 M-600 어플라이언스를 구입하고 구독을 새 어플라이언스로 마이그레이션합니다.

1. 새로운 M-200 또는 M-600 어플라이언스를 구입합니다.
2. 새로운 지원 라이선스와 마이그레이션 라이선스를 구매하세요.
3. 새 M-200 또는 M-600 어플라이언스를 구입할 때 판매 담당자에게 단계적으로 중단하려는 M-100 또는 M-500 어플라이언스의 일련번호 및 디바이스 관리 인증 코드와 선택한 라이선스 마이그레이션 날짜를 제공합니다. M-200 또는 M-600 어플라이언스를 받으면 어플라이언스를

 ©2024 Palo Alto Networks, Inc.

등록하고 Palo Alto Networks에서 제공하는 마이그레이션 및 지원 인증 코드를 사용하여 어플라이언스 관리 및 지원 라이선스를 활성화합니다. 마이그레이션 날짜에 M-100 또는 M-500의 디바이스 관리 라이선스가 해제되며 더 이상 M-100 또는 M-500 어플라이언스를 사용하여 디바이스를 관리하거나 로그를 수집할 수 없습니다. 그러나 지원 라이선스는 유지되고 Panorama 어플라이언스는 계속 지원됩니다. 유효 날짜 이후에 마이그레이션을 완료할 수 있지만 현재 사용 중지된 M-100 또는 M-500 어플라이언스에서 구성 변경 사항을 커밋할 수 없습니다.

Palo Alto Networks는 M 시리즈 어플라이언스 간에 마이그레이션할 때 최대 90일의 마이그레이션 유예 기간을 허용합니다. 마이그레이션에 대한 자세한 내용은 Palo Alto Networks 영업 담당자에게 문의하십시오.

STEP 3 | Panorama 모드에서 각 M-100 또는 M-500 어플라이언스의 Panorama 구성을 내보냅니다.

(HA 구성) 각 M-100 또는 M-500 어플라이언스 HA 피어에서 이 단계를 수행합니다. M-100 또는 M-500 어플라이언스의 HA 우선 순위(기본 또는 보조) 를 추적합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 이름이 지정된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
4. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.

STEP 4 | 전원을 끌 M-100 또는 M-500 어플라이언스 HA 피어의 Panorama 웹 인터페이스에서 **Panorama** > 설정 > 작업 및 **Panorama** 종료를 선택합니다.

(HA 구성) M-100 또는 M-500 어플라이언스 HA 피어 모두에 대해 이 단계를 반복합니다.

STEP 5 | M-200 또는 M-600 어플라이언스의 초기 설정을 수행합니다.

(HA 구성) M-200 또는 M-600 어플라이언스 HA 피어 모두에 대해 이 단계를 반복합니다.

1. M-500 어플라이언스를 랙에 장착합니다. 지침은 M-200 및 M-600 어플라이언스 하드웨어 참조 안내서를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성을 수행하여 라이선스를 활성화하고 업데이트를 설치하는 데 필요한 네트워크 연결을 정의합니다.
3. Panorama를 등록합니다.
4. Panorama 지원 라이선스 활성화.
5. (FIPS-CC만 해당) 일반 모드에서 FIPS-CC 모드로 마이그레이션할 때 라이선스 서버에서 라이선스 키를 검색합니다.
6. 방화벽 관리 라이선스를 활성화합니다. 마이그레이션 라이선스와 연결된 인증 코드를 사용합니다.
7. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. M-100 또는 M-500 어플라이언스와 동일한 버전을 설치합니다.
8. (전용 로그 수집기만 해당) M 시리즈 어플라이언스를 로그 수집기로 설정합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 각 M-100 또는 M-500 어플라이언스에서 내보낸 Panorama 구성 스냅샷을 Panorama 모드(두 HA 피어 모두)의 각 M-200 또는 M-600 어플라이언스로 로드합니다.

(HA 구성) M-200 또는 M-600 어플라이언스 HA 피어 모두에 대해 이 단계를 반복합니다.

속성 편집 테이블 정책 규칙 작성 및 수정 날짜가 업데이트되어 가져온 *Panorama* 구성을 새 *Panorama*에서 커밋한 날짜를 반영합니다. 각 정책 규칙의 범용 고유 식별자(UUID)는 *Panorama* 구성을 마이그레이션할 때 유지됩니다.

관리형 방화벽의 생성 및 수정은 관리형 방화벽에 대한 정책 규칙 사용을 모니터링할 때 영향을 받지 않습니다. 이 데이터는 *Panorama*가 아닌 관리형 방화벽에 로컬로 저장되기 때문입니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 설정 > 작업을 선택합니다.
3. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭합니다.
4. M-200 또는 M-600 어플라이언스와 동일한 HA 우선 순위(기본 또는 보조) 를 가진 M-100 또는 M-500 어플라이언스에서 내보낸 구성 파일을 찾은 다음 확인을 클릭합니다.
5. 명명된 **Panorama** 구성 스냅샷을 로드하고 방금 가져온 구성의 이름을 선택합니다.
6. 암호 해독 키(Panorama의 마스터 키)를 선택하고 확인을 클릭합니다.
7. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.
8. 커밋 > **Panorama**에 커밋을 선택한 다음 커밋을 확인합니다. 계속하기 전에 오류를 해결합니다.
9. Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 7 | Panorama 모드에서 M-200 또는 M-600 어플라이언스 HA 피어 간의 구성을 동기화합니다.

1. 활성 M-200 또는 M-600 어플라이언스의 Panorama 웹 인터페이스에서 대시보드를 선택합니다.
2. 고가용성 위젯에서 피어와 동기화를 클릭합니다.
3. 고가용성 위젯에서 로컬(기본 M-200 어플라이언스)이 활성이고 피어 가 수동이며 실행 중인 구성이 ###되었는지 확인합니다.

STEP 8 | 디바이스 등록 인증 키를 사용하여 추가된 관리형 방화벽과 전용 로그 수집기에 대한 Panorama에 대한 관리 디바이스 연결 복구를 수행합니다.

이는 한 *Panorama* 모델에서 다른 모델로 전환할 때 필요합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | Panorama 모드에서 활성 M-200 또는 M-600 어플라이언스를 방화벽과 동기화하여 방화벽 관리를 재개합니다.

네트워크 중단을 최소화하려면 유지 관리 기간 동안 이 단계를 완료하십시오.

1. 활성 M-200 또는 M-600 어플라이언스에서 **Panorama** > 관리형 디바이스를 선택한 다음 디바이스 상태 열에 방화벽에 대해 ###이 표시되는지 확인합니다.

   이 시점에서 공유 정책(디바이스 그룹) 및 템플릿 열은 방화벽에 대해 ##### ##을 표시합니다.
2. 디바이스 그룹 및 템플릿에 변경 사항을 푸시합니다.
   1. 커밋 > 디바이스에 푸시를 선택한 다음 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 모든 디바이스 그룹, 디바이스 및 네트워크 템플릿 포함을 선택한 다음 확인을 클릭합니다.
   3. 변경 사항을 푸시합니다.
3. **Panorama** > 관리형 디바이스 페이지에서 공유 정책 및 템플릿 열이 방화벽에 동기화됨으로 표시되는지 확인합니다.

다른 *Panorama* 모델로 마이그레이션한 후 *Panorama*와 관리형 방화벽 간에 연결 문제가 발생한 경우 Panorama에 대한 관리되는 디바이스 연결을 복구하여 문제를 해결하십시오.

 ©2024 Palo Alto Networks, Inc.

Panorama 관리 인터페이스 액세스 및 탐색

Panorama는 세 가지 관리 인터페이스를 제공합니다.

- 웹 인터페이스 - Panorama 웹 인터페이스는 방화벽 웹 인터페이스와 모양과 느낌이 비슷합니다. 후자에 익숙하다면 Panorama 웹 인터페이스에서 쉽게 탐색하고 관리 작업을 완료하고 보고서를 생성할 수 있습니다. 이 그래픽 인터페이스를 사용하면 HTTPS를 사용하여 Panorama에 액세스할 수 있으며 관리 작업을 수행하는 가장 좋은 방법입니다. Panorama 웹 인터페이스에 로그인 및 Panorama 웹 인터페이스 탐색을(를) 참조하십시오. Panorama에 대한 HTTP 액세스를 활성화해야 하는 경우 **Panorama** > 설정 > 관리 탭에서 관리 인터페이스 설정을 편집합니다.
- 명령줄 인터페이스**(CLI)** - CLI는 명령을 연속적으로 빠르게 입력하여 일련의 작업을 완료할 수 있게 해주는 단순한 인터페이스입니다. CLI는 작동 및 구성의 두 가지 명령 모드를 지원하며 각각 고유한 명령 및 명령문 계층이 있습니다. 명령의 중첩 구조와 구문에 익숙해지면 CLI를 통해 빠른 응답 시간과 관리 효율성을 얻을 수 있습니다. Panorama CLI에 로그인를 참조하십시오.
- **XML API** - XML 기반 API는 HTTP/HTTPS 요청 및 응답을 사용하여 구현되는 웹 서비스로 제공됩니다. 이를 통해 운영을 간소화하고 기존 내부 개발 애플리케이션 및 리포지토리와 통합할 수 있습니다. Panorama API 사용에 대한 자세한 내용은 PAN-OS 및 Panorama XML API 사용 가이드를 참조하십시오.

Panorama 웹 인터페이스에 로그인

*6*개 이상의 동시 API 호출이 있는 경우, *Panorama* 또는 관리 전용 모드의 *M-600* 어플라이언스에 대한 *Panorama* 웹 인터페이스에 액세스할 수 없습니다. *6*개 이상의 동시 *API* 호출이 있는 *M-600* 어플라이언스의 *Panorama* 웹 인터페이스에 로그인하려고 하면 *504 ##### ## ##* 오류가 표시됩니다.

STEP 1 | 인터넷 브라우저를 실행하고 보안 연결(https://<IP address>)을 사용하여 Panorama IP 주소를 입력합니다.

STEP 2 | 계정에 사용된 인증 유형에 따라 Panorama에 로그인합니다. Panorama에 처음 로그인하는 경우 사용자 이름과 암호에 기본값인 **admin**을 사용합니다.

- **SAML - Single Sign-On(SSO)** 사용을 클릭합니다. Panorama가 관리자에 대한 권한 부여(역할 할당)를 수행하는 경우 사용자 이름을 입력하고 계속하십시오. SAML ID 공급자(IdP)가 권한 부여를 수행하는 경우 사용자 이름을 입력하지 않고 계속합니다. 두 경우 모두 Panorama는 사용자 이름과 암호를 입력하라는 메시지를 표시하는 IdP로 리디렉션합니다. IdP에 인증하면 Panorama 웹 인터페이스가 표시됩니다.
- 다른 유형의 인증 - 사용자 이름과 암호를 입력합니다. 로그인 페이지에 배너와 체크박스가 있는 경우 로그인 배너를 읽고 아래 진술에 동의하고 확인합니다를 선택합니다. 그런 다음 로그인을 클릭합니다.

STEP 3 | 오늘의 모든 메시지를 읽고 닫습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 웹 인터페이스 탐색

Panorama 웹 인터페이스를 사용하여 Panorama를 구성하고 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터를 관리 및 모니터링하고 컨텍스트 드롭다운을 통해 각 방화벽의 웹 인터페이스에 액세스합니다. 각 웹 인터페이스 탭의 옵션 및 필드에 대한 자세한 내용은 Panorama 온라인 도움말을 참조하십시오. 다음은 탭에 대한 개요입니다.

탭	설명
계기반	Panorama 모델 및 네트워크 액세스 설정에 대한 일반 정보를 봅니다. 이 탭에는 애플리케이션, 로그, 시스템 리소스 및 시스템 설정에 대한 정보를 표시하는 위젯이 포함되어 있습니다.
ACC	Panorama가 관리 방화벽에서 수집한 정보를 기반으로 네트워크의 전반적인 위험 및 위협 수준을 확인합니다.
모니터	로그 및 보고서를 보고 관리합니다.
디바이스 그룹 > 선언	중앙 집중식 정책 규칙을 만들어 여러 방화벽/디바이스 그룹에 적용합니다. 이 탭이 표시되도록 디바이스 그룹 추가해야 합니다.
디바이스 그룹 > 개체	정책 규칙이 참조할 수 있고 관리되는 방화벽/디바이스 그룹이 공유할 수 있는 정책 개체를 정의합니다. 이 탭이 표시되도록 디바이스 그룹 추가해야 합니다.
템플릿 > 네트워크	네트워크 프로파일과 같은 네트워크 설정을 구성하고 여러 방화벽에 적용합니다. 이 탭이 표시되도록 템플릿 추가해야 합니다.
템플릿 > 디바이스	서버 프로파일 및 관리자 역할과 같은 디바이스 설정을 구성하고 여러 방화벽에 적용합니다. 이 탭이 표시되도록 템플릿 추가해야 합니다.
Panorama	Panorama를 구성하고, 라이선스를 관리하고, 고가용성을 설정하고, 소프트웨어 업데이트 및 보안 경고에 액세스하고, 관리 액세스를 관리하고, 배포된 방화벽, Log Collector, WildFire 어플라이언스 및 어플라이언스 클러스터를 관리합니다.

Panorama CLI에 로그인

직렬 포트 연결을 사용하거나 SSH(Secure Shell) 클라이언트를 사용하여 원격으로 Panorama CLI에 로그인할 수 있습니다.

©2024 Palo Alto Networks, Inc.

- SSH를 사용하여 Panorama CLI에 로그인합니다.

  동일한 지침이 Log Collector 모드의 M-Series 어플라이언스에 적용됩니다.

  선택적으로 CLI에 대한 SSH 키 기반 인증을 사용하여 관리자 구성을(를) 수행할 수 있습니다.

  1. 다음 전제 조건이 충족되는지 확인합니다.
     - Panorama에 네트워크로 액세스할 수 있는 컴퓨터가 있습니다.
     - Panorama IP 주소를 알고 있습니다.
     - 관리 인터페이스는 기본 설정인 SSH를 지원합니다. 관리자가 SSH를 비활성화했는데 다시 활성화하려면 **Panorama** > **Setup** > **Interfaces**를 선택한 다음 관리를 클릭하고 **SSH**를 선택한 다음 확인을 클릭하고 커밋 > **Panorama**에 커밋을 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.
  2. SSH를 사용하여 CLI에 액세스하려면:
     1. SSH 클라이언트에 Panorama IP 주소를 입력하고 포트 22를 사용합니다.
     2. 메시지가 표시되면 관리 액세스 자격 증명을 입력합니다. 로그인하면 오늘의 메시지가 표시된 후 작동 모드에서 CLI 프롬프트가 표시됩니다. 예:

        ```
        admin@ABC_Sydney>
        ```

- 직렬 포트 연결을 사용하여 Panorama CLI에 로그인합니다.
  1. 다음 사항이 있는지 확인합니다.
     - Panorama를 DB-9 직렬 포트가 있는 컴퓨터에 연결하는 널 모뎀 직렬 케이블
     - 컴퓨터에서 실행되는 터미널 에뮬레이션 프로그램
  2. 터미널 에뮬레이션 소프트웨어에서 다음 설정을 사용하여 연결합니다. 9600 보드, 8 데이터 비트, 1 정지 비트, 패리티 없음, 하드웨어 플로우 제어가 없습니다.
  3. 메시지가 표시되면 관리 액세스 자격 증명을 입력합니다. 로그인하면 오늘의 메시지가 표시된 후 작동 모드에서 CLI 프롬프트가 표시됩니다.

- 구성 모드로 변경합니다.

  구성 모드로 전환하려면 프롬프트에서 다음 명령을 입력하십시오.

  ```
  admin@ABC_Sydney> configure
  ```

  프롬프트가 admin@ABC_Sydney#로 변경됩니다.

 ©2024 Palo Alto Networks, Inc.

Panorama에 대한 관리 액세스 설정

Panorama는 관리자의 권한과 책임을 지정할 수 있도록 역할 기반 액세스 제어(RBAC)을(를) 구현합니다. 다음 주제에서는 Panorama 웹 인터페이스 및 CLI(명령줄 인터페이스)에 액세스하기 위한 관리자 역할, 액세스 도메인 및 계정을 만드는 방법에 대해 설명합니다.

- 관리자 역할 프로파일 구성
- 관리형 방화벽에 대한 선택적 푸시를 위한 관리자 역할 프로파일 구성
- 액세스 도메인 구성
- 관리 계정 및 인증 구성
- 관리자에 대해 SCP 업로드 활성화
- 관리자 활동 추적 구성

관리자 역할 프로파일 구성

관리자 역할 프로파일은 민감한 회사 정보를 보호하고 최종 사용자의 개인 정보를 보호하기 위해 세분화된 관리 액세스 권한을 정의할 수 있는 사용자 지정 관리 역할입니다. 가장 좋은 방법은 관리자가 작업을 수행하는 데 필요한 관리 인터페이스 영역에만 액세스할 수 있도록 하는 관리자 역할 프로파일을 만드는 것입니다.

STEP 1 | 디바이스 > **Admin** 역할을 선택하고 방화벽 관리자 역할 프로파일을 구성할 템플릿을 선택합니다

관리자가 Panorama와 관리 방화벽 웹 인터페이스 간에 컨텍스트 전환을 할 수 있도록 방화벽에서 관리자 역할 프로파일을 생성하고 이를 Panorama 관리 서버 관리자 역할 프로파일에 할당해야 합니다.

STEP 2 | **Panorama** > 관리자 역할을 선택하고 추가를 클릭합니다.

STEP 3 | 프로파일의 이름을 입력하고 역할 유형을 선택합니다. **Panorama** 또는 디바이스 그룹 및 템플릿.

STEP 4 | 아이콘을 원하는 설정으로 전환하여 Panorama(웹 **UI**)의 각 기능 영역에 대한 액세스 권한을 구성합니다. 활성화(읽기-쓰기), 읽기 전용 또는 비활성화합니다.

사용자 지정 역할이 있는 관리자가 관리 방화벽에 대한 디바이스 그룹 또는 템플릿 변경 사항을 커밋하는 경우 해당 역할에 ***Panorama*** > 디바이스 그룹 및 ***Panorama*** > ***Templates***에 대한 읽기-쓰기 액세스 권한을 부여해야 합니다. 이전 *Panorama* 버전에서 업그레이드하는 경우 업그레이드 프로세스는 해당 노드에 대한 읽기 전용 액세스를 제공합니다.

STEP 5 | 역할 유형이 **Panorama**인 경우 각 기능 영역에 대해 활성화/비활성화 아이콘을 전환하여 **XML API**에 대한 액세스를 구성합니다.

STEP 6 | 역할 유형이 **Panorama**인 경우 명령줄 인터페이스에 대한 액세스 수준을 선택합니다. 없음(기본값), 수퍼유저, 수퍼리더 또는 **panorama** 관리자

STEP 7 | (선택 사항) **Panorama** 관리자가 Panorama와 방화벽 웹 인터페이스 간의 컨텍스트 전환을 허용하려면 1단계에서 구성한 디바이스 관리자 역할의 이름을 입력합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 확인을 클릭하여 프로파일을 저장합니다.

관리형 방화벽에 대한 선택적 푸시를 위한 관리자 역할 프로파일 구성

관리 방화벽의 구성 변경 사항을 더 잘 제어하려면 Panorama 관리자가 Panorama™ 관리 서버에서 관리 방화벽으로 한 명 이상의 Panorama 관리자에 대한 구성을 푸시할 수 있도록 관리자 역할 프로파일을 만드십시오. Panorama에 선택적 구성 변경 사항을 커밋한 후 특정 Panorama 관리자 변경 사항을 선택하여 구성 변경 사항을 검토한 다음 선택한 관리자가 변경한 사항만 관리 방화벽에 푸시할 수 있습니다. 관리 방화벽에 대한 선택적 푸시를 활용하면 관리 방화벽에 푸시할 때 불완전한 구성 변경 사항을 명시적으로 제외할 수 있으므로 불완전한 디바이스 그룹 및 템플릿 구성을 관리 방화벽에 푸시할 위험도 줄어듭니다. 이는 네트워크 중단을 유발할 수 있는 잠재적인 중단 및 구성 관련 문제를 완화하고 방지하는 데 도움이 됩니다.

수퍼유저 또는 Panorama 관리자 역할 권한이 있는 관리자는 기본적으로 다른 관리자의 개체 수준 변경 사항을 푸시하고 검토할 수 있습니다. 그러나 Panorama 관리자 역할을 수정하여 필요에 따라 개체 수준 구성 권한을 수정할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | (선택 사항) 디바이스 > **Admin** 역할을 선택하고 방화벽 관리자 역할 프로파일을 구성할 템플릿을 선택합니다.

관리자가 Panorama와 관리 방화벽 웹 인터페이스 간에 컨텍스트 전환을 할 수 있도록 방화벽에서 관리자 역할 프로파일을 생성하고 이를 Panorama 관리 서버 관리자 역할 프로파일에 할당해야 합니다.

STEP 3 | **Panorama** > 관리자 역할을 선택하고 새 관리자 역할을 추가합니다.

STEP 4 | 관리자 역할을 설명하는 이름을 입력합니다.

STEP 5 | **Panorama** 관리자 역할을 선택합니다.

STEP 6 | 웹 **UI**를 선택하고 커밋 권한으로 이동합니다.

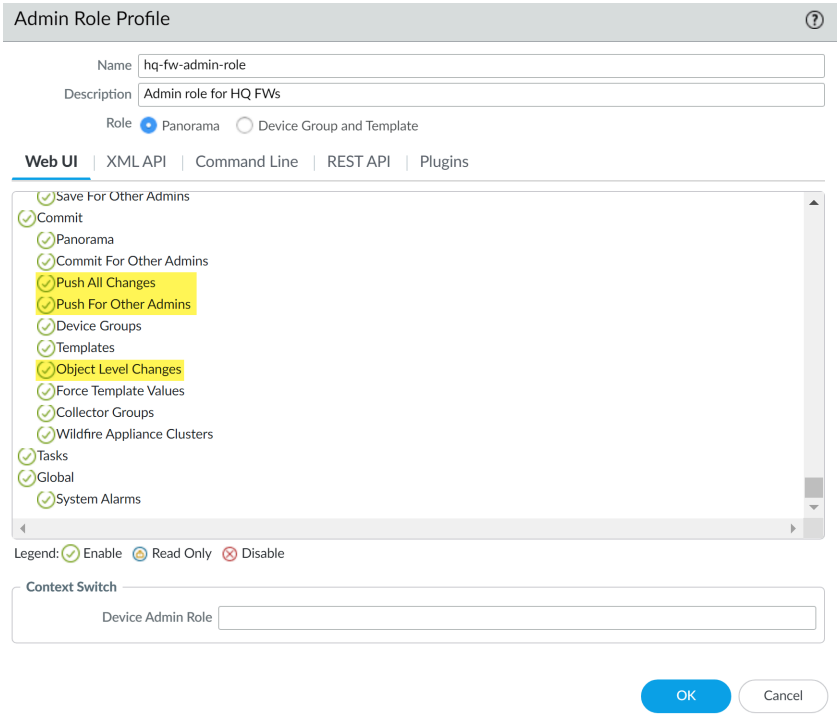
 ©2024 Palo Alto Networks, Inc.

STEP 7 | 필요에 따라 개체 수준 구성 권한을 구성합니다.

모든 개체 수준 구성 권한은 기본적으로 활성화되어 있습니다.

기본 수퍼유저 또는 Panorama 관리자 역할 권한은 전체 개체 수준 구성 권한을 지원합니다.

- 모든 변경 사항 푸시 - 관리자가 모든 관리자가 수행한 모든 변경 사항을 푸시할 수 있습니다.
- 다른 관리자에게 푸시 - 관리자가 다른 관리자가 수행한 구성 변경 사항을 선택하고 푸시할 수 있습니다.
- 개체 수준 변경 - 관리자가 푸시할 개별 구성 개체를 볼 수 있습니다. 비활성화된 경우 구성 개체 목록이 푸시 범위에 표시되지 않습니다.



STEP 8 | (선택 사항) **Panorama** 관리자가 Panorama와 방화벽 웹 인터페이스 간의 컨텍스트 전환을 허용하려면 1단계에서 구성한 디바이스 관리자 역할의 이름을 입력합니다.

STEP 9 | 확인을 클릭합니다.

STEP 10 | 사용자 지정 Panorama 관리자를 구성하고 생성한 관리자 역할을 선택합니다.

STEP 11 | 커밋 및 **Panorama**에 커밋.

액세스 도메인 구성

액세스 도메인을(를) 사용하여 특정 디바이스 그룹 및 템플릿에 대한 디바이스 그룹 및 템플릿 관리자의 액세스를 정의하고 해당 관리자가 컨텍스트를 관리되는 방화벽의 웹 인터페이스로 전환하는 기능을 제어합니다. Panorama는 최대 4,000개의 액세스 도메인을 지원합니다.

STEP 1 | **Panorama** > 액세스 도메인을 선택하고 추가를 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 액세스 도메인을 식별하는 이름을 입력합니다.

STEP 3 | 공유 객체에 대한 액세스 권한 선택:

- 쓰기 - 관리자는 공유 개체에 대한 모든 작업을 수행할 수 있습니다. 이것이 기본값입니다.
- 읽기 - 관리자는 공유 개체를 표시하고 복제할 수 있지만 다른 작업을 수행할 수는 없습니다. 비공유 개체를 추가하거나 공유 개체를 복제할 때 대상은 공유 위치가 아니라 액세스 도메인 내의 디바이스 그룹이어야 합니다.
- 공유 전용 - 관리자는 공유 위치에만 개체를 추가할 수 있습니다. 관리자는 공유 객체를 표시, 편집 및 삭제할 수 있지만 이동하거나 복제할 수는 없습니다.

이 옵션의 결과로 관리자는 비공유 개체를 표시하는 것 외에 다른 작업을 수행할 수 없습니다. 이 옵션을 선택하는 이유는 모든 개체가 단일 글로벌 리포지토리에 있어야 하는 조직의 경우입니다.

STEP 4 | 디바이스 그룹 탭의 아이콘을 토글하여 액세스 도메인의 디바이스 그룹에 대해 읽기-쓰기 또는 읽기 전용 액세스를 활성화합니다.

공유 개체 액세스를 공유 전용으로 설정하면 *Panorama*는 읽기-쓰기 액세스를 지정하는 모든 디바이스 그룹의 개체에 읽기 전용 액세스를 적용합니다.

STEP 5 | 템플릿 탭을 선택하고 액세스 도메인에 할당할 각 템플릿을 추가합니다.

STEP 6 | 디바이스 컨텍스트 탭을 선택하고 액세스 도메인에 할당할 방화벽을 선택한 후 확인을 클릭합니다. 관리자는 Panorama의 컨텍스트 드롭다운을 사용하여 이러한 방화벽의 웹 인터페이스에 액세스할 수 있습니다.

관리 계정 및 인증 구성

인증 프로파일을 이미 구성했거나 관리자를 인증하는 데 프로파일이 필요하지 않은 경우 Panorama 관리자 계정 구성을(를) 준비합니다. 그렇지 않으면 아래 나열된 다른 절차 중 하나를 수행하여 특정 유형의 인증에 대한 관리 계정을 구성합니다.

- Panorama 관리자 계정 구성
- Panorama 관리자에 대한 로컬 또는 외부 인증 구성
- 웹 인터페이스에 대한 인증서 기반 인증으로 Panorama 관리자 구성
- CLI에 대한 SSH 키 기반 인증을 사용하여 관리자 구성
- Panorama 관리자를 위한 RADIUS 인증 구성
- Panorama 관리자를 위한 TACACS+ 인증 구성
- Panorama 관리자를 위한 SAML 인증 구성

Panorama 관리자 계정 구성

관리 계정은 Panorama 관리자에 대한 관리 역할 및 인증을 지정합니다. 역할을 할당하고 인증을 수행하는 데 사용하는 서비스에 따라 Panorama, 외부 서버 또는 둘 다에 계정을 추가할지의 여부가 결정됩니다(관리 인증 참조). 외부 인증 서비스의 경우 관리 계정을 추가하기 전에 인증 프로파일을 구성해야 합니다(관리

 ©2024 Palo Alto Networks, Inc.

계정 및 인증 구성 참조). 인증 프로파일을 이미 구성했거나 Panorama에 로컬인 인증 메커니즘을 사용하려는 경우 다음 단계를 수행하여 Panorama에 관리 계정을 추가합니다.

STEP 1 | 지원되는 관리자 계정 수를 수정합니다.

일반 작동 모드 또는 FIPS-CC 모드에서 Panorama에 대해 지원되는 총 동시 관리 계정 세션 수를 구성합니다. 최대 4개의 동시 관리 계정 세션을 허용하거나 동시 관리 계정 세션을 무제한으로 지원하도록 Panorama를 구성할 수 있습니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 최대 세션 수를 편집하여 모든 관리자 및 사용자 계정에 허용되는 지원되는 동시 세션 수(범위는 **0**~ **4**)를 지정합니다.

   관리 계정을 무제한으로 지원하도록 Panorama를 구성하려면 **0**을 입력합니다.
3. 관리 계정에 대한 최대 세션 시간(분)을 편집합니다. 기본값은 720분입니다.
4. 확인을 클릭합니다.
5. 커밋 및 **Panorama**에 커밋.

Panorama CLI에 로그인하여 지원되는 총 동시 세션 수를 구성할 수도 있습니다.

```
admin> configure
```

```
admin# set deviceconfig setting management admin-session
 max-session-count <0-4>
```

```
admin# set deviceconfig setting management admin-session
 max-session-time <0, 60-1499>
```

```
admin# ##
```

STEP 2 | **Panorama** > 관리자를 선택하고 계정을 추가합니다.

STEP 3 | 관리자의 사용자 이름을 입력합니다.

STEP 4 | 관리자에 대해 구성한 경우 인증 프로파일 또는 시퀀스를 선택합니다.

이는 Panorama가 인증을 위해 Kerberos SSO 또는 외부 서비스를 사용하는 경우 필요합니다.

Panorama가 로컬 인증을 사용하는 경우 인증 프로파일을 없음으로 설정하고 암호를 입력한 다음 암호 확인을 입력합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 관리자 유형을 선택합니다.

- 동적 - 사전 정의된 관리자 역할을 선택합니다.
- **Custom Panorama Admin** - 이 관리자에 대해 생성한 관리자 역할 프로파일을 선택합니다(관리자 역할 프로파일 구성 참조).
- 디바이스 그룹 및 템플릿 관리자 - 다음 단계에 설명된 대로 액세스 도메인을 관리 역할에 매핑합니다.

STEP 6 | (디바이스 그룹 및 템플릿 관리자만 해당) 관리자 역할에 대한 액세스 도메인 섹션에서 추가를 클릭하고 드롭다운에서 액세스 도메인을 선택하고(액세스 도메인 구성 참조) 인접한 관리자 역할 셀을 클릭한 후 관리자 역할 프로파일을 선택합니다.

STEP 7 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 8 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

Panorama 관리자에 대한 로컬 또는 외부 인증 구성

외부 인증 서비스 또는 Panorama에 로컬인 서비스를 사용하여 Panorama에 액세스하는 관리자를 인증할 수 있습니다. 이러한 인증 방법은 관리자에게 사용자 이름 및 암호를 입력하기 위한 로그인 페이지와 같은 하나 이상의 인증 문제에 응답하도록 합니다.

외부 서비스를 사용하여 인증 및 권한 부여(역할 및 도메인 할당에 액세스)를 모두 관리하는 경우 다음을 참조하십시오.

- Panorama 관리자를 위한 RADIUS 인증 구성
- Panorama 관리자를 위한 TACACS+ 인증 구성
- Panorama 관리자를 위한 SAML 인증 구성

시도 응답 메커니즘 없이 관리자를 인증하려면 웹 인터페이스에 대해 인증서 기반 인증을 사용하여 Panorama 관리자를 구성하고 CLI에 대해 SSH 키 기반 인증을 사용하여 관리자를 구성할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (외부 인증만 해당) Panorama를 활성화하여 관리자 인증을 위해 외부 서버에 연결합니다.

1. **Panorama** > 서버 프로파일을 선택하고 서비스 유형(**RADIUS**, **TACACS+**, **SAML**, **LDAP** 또는 **Kerberos**)을 선택하고 서버 프로파일을 구성합니다.

   - Panorama 관리자에 대한 RADIUS 인증을 구성합니다.

     RADIUS 서버를 사용하여 *RADIUS* 인증 서비스 또는 MFA(다단계 인증) 서비스를 지원할 수 있습니다.

   - Panorama 관리자를 위한 TACACS+ 인증을 구성합니다.
   - SAML IdP 서버 프로파일을 추가합니다. Kerberos SSO(Single Sign-On)를 SAML SSO와 결합할 수 없습니다. 한 가지 유형의 SSO 서비스만 사용할 수 있습니다.
   - Kerberos 서버 프로파일을 추가합니다.
   - LDAP 서버 프로파일을 추가합니다.

STEP 2 | (선택 사항) Panorama가 로컬 인증을 사용하는 경우 암호 복잡성 및 만료 설정을 정의합니다.

이러한 설정은 공격자가 암호를 추측하기 어렵게 하여 무단 액세스로부터 Panorama를 보호하는 데 도움이 됩니다.

1. 모든 로컬 관리자에 대한 글로벌 암호 복잡성 및 만료 설정을 정의합니다.

   1. **Panorama** > **Setup** > **Management**를 선택하고 최소 암호 복잡성 설정을 편집합니다.
   2. 사용을 선택합니다.
   3. 암호 설정을 정의하고 확인을 클릭합니다.

2. 암호 프로파일을 정의합니다.

   전역 암호 만료 설정을 재정의하려는 관리자 계정에 프로파일을 할당합니다.

   1. **Panorama** > 암호 프로파일을 선택하고 프로파일을 추가합니다.
   2. 프로파일을 식별할 이름을 입력합니다.
   3. 암호 만료 설정을 정의하고 확인을 클릭합니다.

STEP 3 | (Kerberos SSO만) Kerberos 키탭을 생성합니다.

keytab은 Panorama에 대한 Kerberos 계정 정보가 포함된 파일입니다. Kerberos SSO를 지원하려면 네트워크에 Kerberos 인프라가 있어야 합니다.

STEP 4 | 인증 프로파일을 구성합니다.

관리 계정이 여러 유형의 서버에 저장되어 있는 경우 각 유형에 대한 인증 프로파일을 생성하고 모든 프로파일을 인증 순서에 추가할 수 있습니다.

인증 프로파일에서 인증 서비스 유형 및 관련 설정을 지정합니다.

- 외부 서비스 - 외부 서비스 유형을 선택하고 생성한 서버 프로파일을 선택합니다.
- 로컬 인증 - 유형을 없음으로 설정합니다.
- **Kerberos SSO** - **Kerberos** 영역을 지정하고 생성한 **Kerberos Keytab**을 가져옵니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (디바이스 그룹 및 템플릿 관리자만 해당) 액세스 도메인을 구성합니다.

하나 이상의 액세스 도메인을 구성합니다.

STEP 6 | (사용자 지정 역할만 해당) 관리자 역할 프로파일을 구성합니다.

하나 이상의 관리자 역할 프로파일을 구성합니다.

사용자 정의 Panorama 관리자의 경우 프로파일은 계정에 대한 액세스 권한을 정의합니다. 디바이스 그룹 및 템플릿 관리자의 경우 프로파일은 계정과 연결된 하나 이상의 액세스 도메인에 대한 액세스 권한을 정의합니다.

STEP 7 | 관리자를 구성합니다.

1. Panorama 관리자 계정을 구성합니다.
   - 구성한 인증 프로파일 또는 시퀀스를 할당합니다.
   - (디바이스 그룹 및 템플릿 관리자만 해당) 액세스 도메인을 관리자 역할 프로파일에 매핑합니다.
   - (로컬 인증만 해당) 암호 프로파일을 구성한 경우 이를 선택합니다.
2. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.
3. (선택 사항) 인증 서버 연결을 테스트하여 Panorama가 인증 프로파일을 사용하여 관리자를 인증할 수 있는지 확인합니다.

웹 인터페이스에 대한 인증서 기반 인증으로 Panorama 관리자 구성

Panorama 웹 인터페이스에 대한 암호 기반 인증에 대한 보다 안전한 대안으로 Panorama에 로컬인 관리자 계정에 대한 인증서 기반 인증을 구성할 수 있습니다. 인증서 기반 인증에는 암호 대신 디지털 서명의 교환 및 확인이 포함됩니다.



모든 관리자에 대해 인증서 기반 인증을 구성하면 *Panorama*의 모든 관리자에 대한 사용자 이름/비밀번호 로그인이 비활성화되고 이후 모든 관리자는 로그인할 인증서가 필요합니다.

STEP 1 | Panorama에서 인증 기관(CA) 인증서를 생성합니다.

이 CA 인증서를 사용하여 각 관리자의 클라이언트 인증서에 서명합니다.

자체 서명된 루트 CA 인증서를 생성합니다.



또는 엔터프라이즈 CA에서 인증서를 가져올 수 있습니다.

STEP 2 | 웹 인터페이스에 대한 액세스를 보호하기 위해 인증서 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택하고 추가를 클릭합니다.
2. 인증서 프로파일의 이름을 입력하고 사용자 이름 필드를 제목으로 설정합니다.
3. CA 인증서 섹션에서 추가를 선택하고 방금 생성한 **CA** 인증서를 선택합니다.
4. 확인을 클릭하여 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 관리자 인증에 인증서 프로파일을 사용하도록 Panorama를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택하고 인증 설정을 편집합니다.
2. 방금 생성한 인증서 프로파일을 선택하고 확인을 클릭합니다.

STEP 4 | 클라이언트 인증서 인증을 사용하도록 관리자 계정을 구성합니다.

Panorama 웹 인터페이스에 액세스할 각 관리자에 대한 Panorama 관리자 계정 구성. 클라이언트 인증서 인증(웹)만 사용 확인란을 선택합니다.

엔터프라이즈 CA에서 생성한 클라이언트 인증서를 이미 배포한 경우 8단계로 건너뜁니다. 그렇지 않으면 5단계를 계속하십시오.

STEP 5 | 각 관리자에 대한 클라이언트 인증서를 생성합니다.

Panorama에서 인증서를 생성합니다. 서명자 드롭다운에서 생성한 CA 인증서를 선택합니다.

STEP 6 | 클라이언트 인증서를 내보냅니다.

1. 인증서를 내보냅니다.
2. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

   Panorama는 로그인 세션을 다시 시작하고 종료합니다. 그 이후에는 관리자가 생성한 클라이언트 인증서가 있는 클라이언트 시스템에서만 웹 인터페이스에 액세스할 수 있습니다.

STEP 7 | 웹 인터페이스에 액세스할 각 관리자의 클라이언트 시스템으로 클라이언트 인증서를 가져옵니다.

이 단계를 완료하려면 필요에 따라 웹 브라우저 설명서를 참조하십시오.

STEP 8 | 관리자가 웹 인터페이스에 액세스할 수 있는지 확인하십시오.

1. 클라이언트 인증서가 있는 컴퓨터의 브라우저에서 Panorama IP 주소를 엽니다.
2. 메시지가 표시되면 불러온 인증서를 선택한 다음 확인을 클릭합니다. 브라우저에 인증서 경고가 표시됩니다.
3. 브라우저 예외 목록에 인증서를 추가합니다.
4. 로그인을 클릭합니다. 웹 인터페이스는 사용자 이름이나 암호를 묻는 메시지 없이 나타나야 합니다.

CLI에 대한 SSH 키 기반 인증을 사용하여 관리자 구성

SSH(Secure Shell)를 사용하여 Panorama CLI에 액세스하는 관리자의 경우 SSH 키는 암호보다 더 안전한 인증 방법을 제공합니다. SSH 키는 무차별 대입 공격의 위험을 거의 제거하고 이중 인증 옵션(개인 키 및 암호)을 제공하며 네트워크를 통해 암호를 보내지 않습니다. 또한 SSH 키를 사용하면 자동화된 스크립트가 CLI에 액세스할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | SSH 키 생성 도구를 사용하여 관리자의 클라이언트 시스템에서 비대칭 키 쌍을 생성합니다.

지원되는 키 형식은 IETF SECSH 및 Open SSH입니다. 지원되는 알고리즘은 DSA(1024비트) 및 RSA(768-4096비트)입니다.

키 쌍을 생성하는 명령은 SSH 클라이언트 설명서를 참조하십시오.

공개 키와 개인 키는 별도의 파일입니다. Panorama가 액세스할 수 있는 위치에 둘 다 저장합니다. 보안 강화를 위해 암호를 입력하여 개인 키를 암호화합니다. Panorama는 로그인하는 동안 관리자에게 이 암호를 입력하라는 메시지를 표시합니다.

STEP 2 | 공개 키 인증을 사용하도록 관리자 계정을 구성합니다.

1. Panorama 관리자 계정 구성.
   - SSH 키 인증이 실패할 경우 폴백으로 사용할 두 가지 인증 방법 중 하나를 구성합니다.

     외부 인증 서비스 - 인증 프로파일을 선택합니다.

     로컬 인증 - 인증 프로파일을 없음으로 설정하고 암호 및 암호 확인을 입력합니다.
   - 공개 키 인증**(SSH)** 사용 확인란을 선택하고 키 가져오기를 클릭하고 방금 생성한 공개 키를 찾아 확인을 클릭합니다.
2. 확인을 클릭하여 관리 계정을 저장합니다.
3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 3 | 개인 키를 사용하여 Panorama에 인증하도록 SSH 클라이언트를 구성합니다.

관리자의 클라이언트 시스템에서 이 작업을 수행합니다. 이 단계를 완료하려면 SSH 클라이언트 설명서를 참조하십시오.

STEP 4 | 관리자가 SSH 키 인증을 사용하여 Panorama CLI에 액세스할 수 있는지 확인합니다.

1. 관리자의 클라이언트 시스템에서 브라우저를 사용하여 Panorama IP 주소로 이동합니다.
2. Panorama CLI에 관리자로 로그인합니다. 사용자 이름을 입력하면 다음 출력이 표시됩니다(키 값은 예시임).

   ```
   ## ## ## "dsa-key-20130415"
   ```
3. 메시지가 표시되면 키를 생성할 때 정의한 암호를 입력합니다.

Panorama 관리자를 위한 RADIUS 인증 구성

RADIUS 서버를 사용하여 Panorama 웹 인터페이스에 대한 관리 액세스를 인증할 수 있습니다. RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

 ©2024 Palo Alto Networks, Inc.

RADIUS 서버를 사용하여 *Panorama* 웹 인터페이스에 대한 관리 액세스를 인증할 수 있습니다. *RADIUS* 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. *VSA*를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 *Panorama*에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

Palo Alto Networks RADIUS 사전을 *RADIUS* 서버로 가져와 *Panorama*와 *RADIUS* 서버 간의 통신에 필요한 인증 속성을 정의할 수 있습니다.

RADIUS 서버를 사용하여 관리자를 위한 MFA(다단계 인증)를 구현할 수도 있습니다.

STEP 1 | RADIUS 서버 프로파일을 추가합니다.

프로파일은 Panorama가 RADIUS 서버에 연결하는 방법을 정의합니다.

1. **Panorama** > **Server Profiles** > **RADIUS**를 선택하고 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).

   서버 프로파일을 사용하여 *Panorama*를 *MFA* 서비스와 통합하는 경우 관리자에게 인증 질문에 응답할 수 있는 충분한 시간을 제공하는 간격을 입력합니다. 예를 들어 *MFA* 서비스에서 *OTP*(일회성 암호)를 입력하라는 메시지가 표시되면 관리자는 엔드포인트 디바이스에서 *OTP*를 확인한 다음 *MFA* 로그인 페이지에 *OTP*를 입력해야 합니다.
4. Panorama가 RADIUS 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

   RADIUS 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.
5. 각 RADIUS 서버를 추가하고 다음을 입력합니다.
   - 서버를 식별하는 이름
   - **RADIUS** 서버 IP 주소 또는 FQDN
   - **Secret**/**Confirm Secret**(사용자 이름과 암호를 암호화하는 키)
   - 인증 요청을 위한 서버 포트(기본값은 1812)
6. 확인을 클릭하여 서버 프로파일을 저장합니다.

STEP 2 | RADIUS 서버 프로파일을 인증 프로파일에 할당합니다.

인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 인증 프로파일을 식별할 이름을 입력합니다.
3. 유형을 **RADIUS**로 설정합니다.
4. 구성한 서버 프로파일을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

5. **RADIUS**에서 사용자 그룹 검색을 선택하여 RADIUS 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.

   Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
7. 확인을 클릭하여 인증 프로파일을 저장합니다.

STEP 3 | 모든 관리자에 대해 인증 프로파일을 사용하도록 Panorama를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 구성한 인증 프로파일을 선택한 다음 확인을 클릭합니다.

STEP 4 | 관리자에 대한 권한 부여 설정을 정의하는 역할 및 액세스 도메인을 구성합니다.

1. 관리자가 사전 정의된(동적) 역할 대신 사용자 지정 역할을 사용하는 경우 관리자 역할 프로파일을 구성합니다.
2. 관리자가 디바이스 그룹 및 템플릿 역할을 사용하는 경우 액세스 도메인을 구성합니다.

STEP 5 | 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

STEP 6 | RADIUS 서버를 구성합니다.

다음 단계를 수행할 특정 지침은 RADIUS 서버 설명서를 참조하십시오.

1. Panorama IP 주소 또는 호스트 이름을 RADIUS 클라이언트로 추가합니다.
2. 관리자 계정을 추가합니다.

   RADIUS 서버 프로파일이 ***CHAP***를 인증 프로토콜로 지정하는 경우 가역적으로 암호화된 암호로 계정을 정의해야 합니다. 그렇지 않으면 *CHAP* 인증이 실패합니다.
3. Panorama(25461)에 대한 공급업체 코드를 정의하고 각 관리자의 역할, 액세스 도메인 및 사용자 그룹에 대한 RADIUS VSA를 정의합니다.

   사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 하위 사례를 사용하여 역할을 지정합니다(예: **SuperUser**가 아닌 ## ###를 입력).

STEP 7 | RADIUS 서버가 관리자에 대한 인증 및 권한을 수행하는지 확인합니다.

1. RADIUS 서버에 추가한 관리자 계정을 사용하여 Panorama 웹 인터페이스에 로그인합니다.
2. 관리자와 연결된 역할에 대해 허용되는 웹 인터페이스 페이지만 액세스할 수 있는지 확인합니다.
3. 모니터, 정책 및 개체 탭에서 관리자와 연결한 액세스 도메인에 대해 허용된 디바이스 그룹에만 액세스할 수 있는지 확인합니다.

Panorama 관리자를 위한 TACACS+ 인증 구성

TACACS+ 서버를 사용하여 Panorama 웹 인터페이스에 대한 관리 액세스를 인증할 수 있습니다. TACACS+ 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | TACACS+ 서버 프로파일을 추가합니다.

프로파일은 Panorama가 TACACS+ 서버에 연결하는 방법을 정의합니다.

1. **Panorama** > **Server Profiles** > **TACACS+**를 선택한 다음 프로파일을 추가합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).
4. Panorama가 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

   TACACS+ 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.
5. 각 TACACS+ 서버를 추가하고 다음을 입력합니다.
   - 서버를 식별하는 이름
   - **TACACS+** 서버 IP 주소 또는 FQDN
   - **Secret/Confirm Secret**(사용자 이름과 암호를 암호화하는 키)
   - 인증 요청을 위한 서버 포트(기본값: 49)
6. 확인을 클릭하여 서버 프로파일을 저장합니다.

STEP 2 | TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 유형을 **TACACS+**로 설정합니다.
4. 구성한 서버 프로파일을 선택합니다.
5. TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집하려면 TACACS+에서 사용자 그룹 검색을 선택합니다.

   Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
7. 확인을 클릭하여 인증 프로파일을 저장합니다.

STEP 3 | 모든 관리자에 대해 인증 프로파일을 사용하도록 Panorama를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 인증 설정을 편집합니다.
2. 구성한 인증 프로파일을 선택한 다음 확인을 클릭합니다.

STEP 4 | 관리자에 대한 권한 부여 설정을 정의하는 역할 및 액세스 도메인을 구성합니다.

1. 관리자가 사전 정의된(동적) 역할 대신 사용자 지정 역할을 사용하는 경우 관리자 역할 프로파일을 구성합니다.
2. 관리자가 디바이스 그룹 및 템플릿 역할을 사용하는 경우 액세스 도메인을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

STEP 6 | 관리자를 인증하고 권한을 부여하도록 TACACS+ 서버를 구성합니다.

다음 단계를 수행하기 위한 특정 지침은 TACACS+ 서버 설명서를 참조하십시오.

1. Panorama IP 주소 또는 호스트 이름을 TACACS+ 클라이언트로 추가합니다.
2. 관리자 계정을 추가합니다.

   인증 프로토콜로 ***CHAP***를 선택한 경우 역으로 암호화된 암호로 계정을 정의해야 합니다. 그렇지 않으면 *CHAP* 인증이 실패합니다.
3. 각 관리자의 역할, 액세스 도메인 및 사용자 그룹에 대해 TACACS+ VSA를 정의합니다.

   사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 하위 사례를 사용하여 역할을 지정합니다(예: ***SuperUser***가 아닌 *## ###*를 입력).

STEP 7 | TACACS+ 서버가 관리자에 대한 인증 및 권한 부여를 수행하는지 확인합니다.

1. TACACS+ 서버에 추가한 관리자 계정을 사용하여 Panorama 웹 인터페이스에 로그인합니다.
2. 관리자와 연결된 역할에 대해 허용되는 웹 인터페이스 페이지만 액세스할 수 있는지 확인합니다.
3. 모니터, 정책 및 개체 탭에서 관리자와 연결된 액세스 도메인에 대해 허용되는 가상 시스템만 액세스할 수 있는지 확인합니다.

Panorama 관리자를 위한 SAML 인증 구성

Panorama 웹 인터페이스(CLI 제외)에 대한 관리 액세스를 위해 SAML(Security Assertion Markup Language) 2.0을 사용할 수 있습니다. SAML 속성을 사용하여 관리자 권한 부여를 관리할 수도 있습니다. SAML 속성을 사용하면 Panorama에서 설정을 재구성하는 대신 디렉터리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 빠르게 변경할 수 있습니다.

SAML SSO(Single Sign-On) 및 SLO(Single Logout)를 구성하려면 Panorama와 IdP(Identity Provider)를 서로 등록하여 통신을 활성화해야 합니다. IdP가 등록 정보가 포함된 메타데이터 파일을 제공하는 경우 Panorama로 가져와 IdP를 등록하고 IdP 서버 프로파일을 생성할 수 있습니다. 서버 프로파일은 IdP에 연결하는 방법을 정의하고 IdP가 SAML 메시지에 서명하는 데 사용하는 인증서를 지정합니다. Panorama용 인증서를 사용하여 SAML 메시지에 서명할 수도 있습니다. 인증서 사용은 선택 사항이지만 Panorama와 IdP 간의 통신 보안을 위해 권장됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | (권장) IdP 및 Panorama가 SAML 메시지 서명에 사용할 인증서를 얻습니다.

인증서가 키 사용 속성을 지정하지 않으면 서명 메시지를 포함한 모든 사용이 기본적으로 허용됩니다. 이 경우 모든 방법으로 인증서를 얻을 수 있습니다.

인증서가 키 사용 속성을 지정하는 경우 속성 중 하나는 Panorama에서 생성한 인증서에서 사용할 수 없는 디지털 서명이어야 합니다. 이 경우 인증서를 가져와야 합니다.

- **Certificate Panorama**가 **SAML** 메시지에 서명하는 데 사용 - 엔터프라이즈 CA(인증 기관) 또는 타사 CA에서 인증서를 가져옵니다.
- **IdP**가 **SAML** 메시지에 서명하는 데 사용하는 인증서 - IdP에서 인증서가 포함된 메타데이터 파일을 가져옵니다(다음 단계 참조). IdP 인증서는 다음 알고리즘으로 제한됩니다.
  - 공개 키 알고리즘 - RSA(1,024비트 이상) 및 ECDSA(모든 크기).
  - 서명 알고리즘 - SHA1, SHA256, SHA384 및 SHA512.

STEP 2 | SAML IdP 서버 프로파일을 추가합니다.

서버 프로파일은 IdP를 Panorama에 등록하고 연결 방법을 정의합니다.

이 예에서는 Panorama가 자동으로 서버 프로파일을 생성하고 연결, 등록 및 IdP 인증서 정보를 채울 수 있도록 IdP에서 SAML 메타데이터 파일을 가져옵니다.

*IdP*가 메타데이터 파일을 제공하지 않는 경우 ***Panorama*** > ***Server Profiles*** > ***SAML IDP*** 공급자, 서버 프로파일 추가를 선택한 다음 정보를 수동으로 입력합니다(값은 *IdP* 관리자에게 문의).

1. IdP에서 Panorama가 액세스할 수 있는 클라이언트 시스템으로 SAML 메타데이터 파일을 내보냅니다.

   파일에 지정된 인증서는 이전 단계에 나열된 요구 사항을 충족해야 합니다. 파일 내보내기에 대한 지침은 IdP 설명서를 참조하십시오.
2. **Panorama** > 서버 프로파일 > **SAML IDP** 공급자를 선택한 다음 메타데이터 파일을 Panorama로 가져옵니다.
3. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
4. **IDP** 공급자 메타데이터 파일을 찾습니다.
5. (권장) Panorama가 **IdP** 인증서를 검증하도록 하려면 **IdP** 인증서 확인(기본값)을 선택합니다.

   유효성 검사는 인증 프로파일에 서버 프로파일을 할당하고 커밋한 후에만 발생합니다. Panorama는 인증 프로파일의 인증서 프로파일을 사용하여 인증서의 유효성을 검사합니다.

   인증서 유효성 검사는 보안 향상을 위한 모범 사례입니다.
6. Panorama가 IdP 메시지를 검증하는 순간 IdP와 Panorama의 시스템 시간 사이에 허용되는 초 단위의 차이인 **Maximum Clock Skew**를 입력합니다(기본값은 60, 범위는 1~900). 차이가 이 값을 초과하면 인증이 실패합니다.
7. 확인을 클릭하여 서버 프로파일을 저장합니다.
8. 서버 프로파일 이름을 클릭하여 프로파일 설정을 표시합니다. 불러온 정보가 올바른지 확인하고 필요한 경우 편집하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 인증 프로파일을 구성합니다.

인증 프로파일은 SAML IdP 서버 프로파일을 지정하고 SLO와 같은 인증 프로세스에 대한 옵션을 정의합니다.

1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 유형을 **SAML**로 설정합니다.
4. 구성한 **IdP** 서버 프로파일을 선택합니다.
5. 서명 요청에 대한 인증서를 선택합니다.

   Panorama는 이 인증서를 사용하여 IdP에 보내는 메시지에 서명합니다.
6. (선택 사항) 싱글 로그아웃을 활성화합니다(기본적으로 비활성화되어 있음).
7. Panorama가 **ID** 공급자 인증서를 확인하는 데 사용할 인증서 프로파일을 선택합니다.
8. IdP 메시지가 사용자를 식별하는 데 사용하는 사용자 이름 속성을 입력합니다(기본 ### ##).

   사용자에 대한 동적 관리자 역할을 사전 정의하는 경우 하위 사례를 사용하여 역할을 지정합니다(예: ***SuperUser***가 아닌 *## ###*를 입력*). IdP ID* 저장소를 통해 관리자 권한 부여를 관리하는 경우 관리자 역할 속성 및 액세스 도메인 속성도 지정하십시오.
9. 고급을 선택한 다음 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
10. 확인을 클릭하여 인증 프로파일을 저장합니다.

STEP 4 | 모든 관리자에 대해 인증 프로파일을 사용하도록 Panorama를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 인증 설정을 편집한 다음 구성한 인증 프로파일을 선택합니다.
2. 커밋 > **Panorama**에 커밋을 선택하여 Panorama에서 변경 사항을 활성화하고 SAML IdP 서버 프로파일에 할당한 **ID** 공급자 인증서를 확인합니다.

STEP 5 | SAML 메타데이터 파일을 생성하여 IdP에 Panorama를 등록합니다.

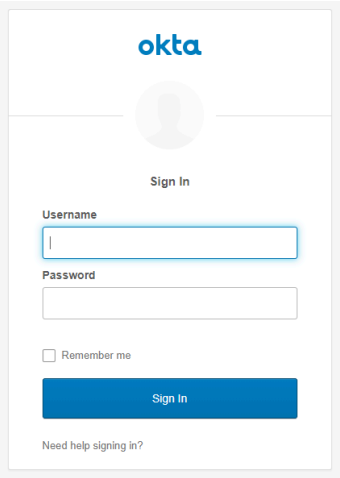
1. **Panorama** > 인증 프로파일을 선택한 다음 구성한 인증 프로파일의 인증 열에서 메타데이터를 클릭합니다.
2. 관리 선택을 인터페이스로 설정하고(기본값이 선택됨) 관리(MGT) 인터페이스를 선택합니다.
3. 확인을 클릭하고 메타데이터 파일을 클라이언트 시스템에 저장합니다.
4. 메타데이터 파일을 IdP 서버로 가져와 Panorama를 등록합니다. 지침은 IdP 설명서를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 관리자가 SAML SSO를 사용하여 인증할 수 있는지 확인합니다.

1. Panorama 웹 인터페이스의 URL로 이동합니다.
2. **Single Sign-On(SSO)** 사용을 클릭합니다.
3. 계속을 클릭합니다.

   Panorama는 로그인 페이지를 표시하는 IdP에 인증하도록 리디렉션합니다. 예:



4. SSO 사용자 이름과 암호를 사용하여 로그인합니다.

   IdP에서 성공적으로 인증하면 웹 인터페이스를 표시하는 Panorama로 다시 리디렉션됩니다.
5. Panorama 관리자 계정을 사용하여 다른 SSO 애플리케이션에 대한 액세스를 요청하십시오.

   액세스 성공은 SAML SSO 인증이 성공했음을 나타냅니다.

관리자에 대해 SCP 업로드 활성화

Panorama™ 관리 서버에서 수퍼유저 관리자가 PAN-OS 소프트웨어 업데이트, 동적 콘텐츠 업데이트, 로컬 디바이스에서 Panorama로 구성 파일 가져오기 등의 지원되는 파일을 업로드할 수 있도록 SCP(Secure Protocol Copy) 사용을 활성화합니다. 이렇게 하면 Panorama 웹 인터페이스를 사용하여 업로드하는 대신 CLI를 사용하여 지원되는 파일 업로드를 자동화할 수 있습니다.

Panorama에 SCP를 성공적으로 전송하거나 어떤 이유로든 SCP 업로드에 실패하면 시스템 로그가 생성됩니다.

Palo Alto Networks는 PAN-OS 소프트웨어 버전, PAN-OS 소프트웨어 변경, 동적 콘텐츠 업데이트, PAN-OS 플러그인 버전, 구성 파일 및 라이선스 키 파일의 SCP 업로드를 지원합니다.

관리형 방화벽의 소프트웨어 업데이트와 동적 콘텐츠 업데이트를 위해 *Panorama*에 *SCP* 업로드를 수행하는 작업은 지원되지 않습니다. 각 개별 방화벽에 대해 소프트웨어 업데이트 또는 동적 콘텐츠 업데이트를 업로드하려면 로컬에서 SCP 업로드를 활성화해야 합니다.

STEP 1 | (선택 사항) SCP 기능을 사용하려면 수퍼유저 권한을 가진 Panorama 관리자를 구성합니다.

이 예에서는 `scp_admin`이라는 수퍼유저 Panorama 관리자를 생성했습니다.

STEP 2 | Panorama CLI에 로그인.

©2024 Palo Alto Networks, Inc.

STEP 3 | 수퍼유저 관리자의 SCP 기능을 활성화합니다.

SCP를 시작하는 관리자는 수퍼유저 권한이 있어야 합니다.

이 예에서는 이전 단계에서 생성한 전용 수퍼유저 `scp_admin`에 대해 SCP 기능을 활성화했습니다.

1. 구성 모드로 전환합니다.

```
admin>configure
```

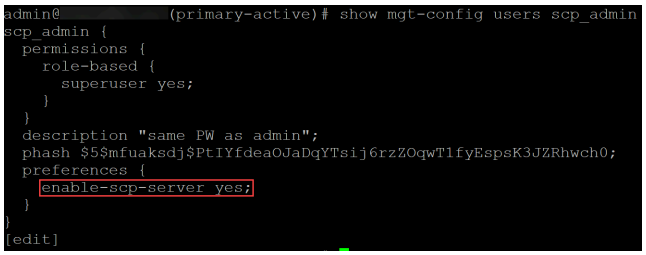
2. 수퍼유저 관리자의 SCP 기능을 활성화합니다.

```
admin#set mgt-config users <admin_name> preferences enable-scp-server yes
```

3. 수퍼유저 관리자의 SCP 기능이 성공적으로 활성화되었는지 확인합니다.

```
admin#show mgt-config users <admin_name>
```

`permissions`에서 `enable-scp-server`에 `yes`가 표시되는지 확인합니다.



4. 커밋합니다.

```
admin# commit
```

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama에 SCP 업로드를 수행합니다.

SCP를 사용하여 Panorama에 파일을 업로드하려면 업로드하는 로컬 디바이스와 Panorama가 동일한 서브넷에 있어야 합니다. 이 단계에서는 로컬 디바이스에서 Panorama에 업로드하려는 파일을 이미 사용할 수 있다고 가정합니다.

이 예에서는 Panorama에 애플리케이션과 위협 콘텐츠 업데이트를 업로드하는 방법을 보여줍니다. 다음은 SCP 업로드를 위해 사전 정의된 대상 디렉터리입니다.

- **PAN-OS** 소프트웨어 버전 — **/scp/software/**
- **PAN-OS** 소프트웨어 패치 — **/scp/patch/**
- 애플리케이션 및 위협 콘텐츠 업데이트 — **/scp/content/**
- **WildFire** 콘텐츠 업데이트 — **/scp/wildfire/**
- 안티바이러스 콘텐츠 업데이트 — **/scp/anti-virus/**
- **PAN-OS** 플러그인 버전 — **/scp/plugin/**
- **XML** 구성 파일 — **/scp/config/**

  성공적으로 *SCP*를 업로드하려면 모든 *PAN-OS* 구성 파일의 파일 이름에 *.xml* 확장자가 추가되어야 합니다.
- 라이선스 키 파일 — **/scp/license/**

1. CLI 터미널을 열고 **cd** 명령을 사용하여 SCP로 보내려는 파일이 있는 폴더 또는 디렉터리로 이동합니다.

   올바른 폴더 또는 디렉터리로 이동한 후 **ls**를 입력하여 폴더 또는 디렉터리 콘텐츠를 확인합니다.

   이 예에서는 Panorama에 업로드할 `panupv2-all-contents-8765-8342` 파일을 볼 수 있습니다.
2. SCP 지원 수퍼유저 관리자를 사용하여 Panorama에 파일을 업로드합니다.

   WinSCP 및 *FileZilla*와 같은 *SCP* 애플리케이션은 지원되지 않습니다. *SCP* 명령은 디바이스 명령줄에서 실행해야 합니다.

   - **OpenSSH 8** 또는 이전 버전을 실행하는 운영 체제

     ```
     scp <file_name> <scp_superuser>@<panorama_IP>:/scp/
     <file_type>/<file_name>
     ```

     `scp_admin`을 사용하여 애플리케이션 및 위협 콘텐츠 업데이트를 업로드하기 위한 SCP 명령의 예입니다.

     ```
     scp panupv2-all-contents-8765-8342 scp_admin@<panorama_IP>:/
     scp/content/panupv2-all-contents-8765-8342
     ```


©2024 Palo Alto Networks, Inc.

- **OpenSSH 9** 이상을 실행하는 운영 체제

```
 scp -o <file_name> <scp_superuser>@<panorama_IP>:/scp/
<file_type>/<file_name>
```

`scp_admin`을 사용하여 애플리케이션 및 위협 콘텐츠 업데이트를 업로드하기 위한 SCP 명령의 예입니다.

```
scp -o panupv2-all-contents-8765-8342
 scp_admin@<panorama_IP>:/scp/content/panupv2-all-
contents-8765-8342
```

3. Panorama 인증을 확인하라는 메시지가 표시되면 **yes**를 입력합니다.

   이 디바이스에서 SSH를 사용하여 Panorama에 이미 연결한 경우 인증을 확인하라는 메시지가 표시되지 않으며 이 단계를 건너뛰어도 됩니다.

4. 메시지가 표시되면 SCP 관리자 ##를 입력하고 Enter를 클릭하여 계속합니다.
5. SCP 업로드 진행 상황이 표시됩니다.

   진행 상태가 `100%`로 표시되고 CLI 명령 프롬프트를 사용할 수 있게 되면 SCP 업로드가 완료된 것입니다.



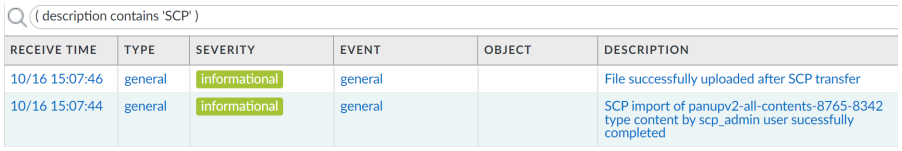
 ©2024 Palo Alto Networks, Inc.

STEP 5 | SCP 업로드를 확인합니다.

생성된 시스템 로그를 검토하여 SCP 업로드가 성공했는지 확인하고 업로드된 파일을 사용할 수 있는지 확인할 수 있습니다. 이 예에서는 애플리케이션 및 위협 콘텐츠 업데이트 버전 8765-8342의 SCP 업로드에 대한 시스템 로그를 검토합니다.

1. Panorama 웹 인터페이스에 로그인.
2. 모니터 > 시스템을 선택하고 SCP 업로드를 필터링합니다.

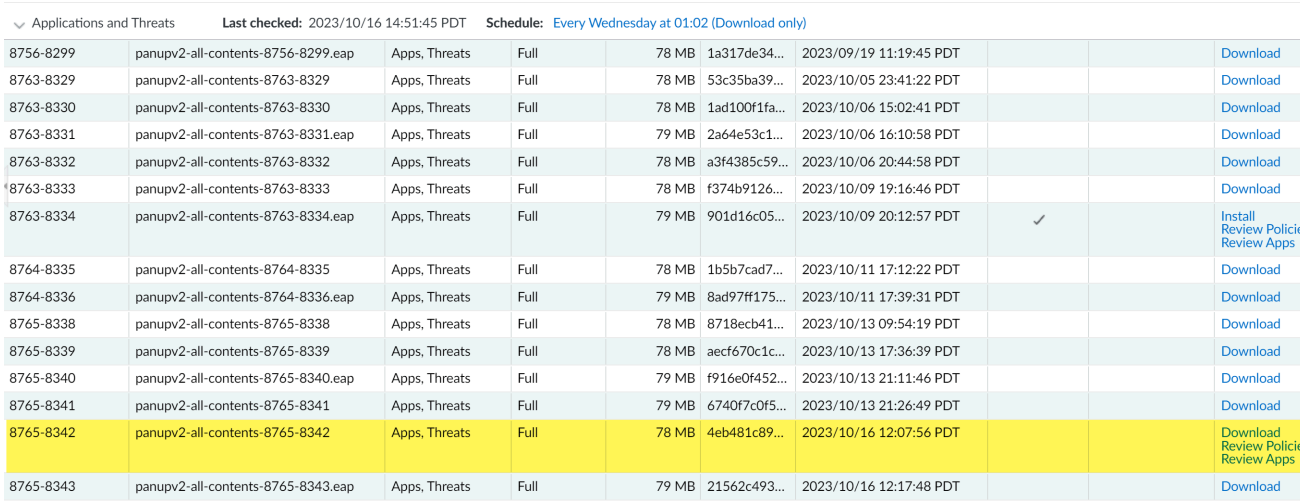
```
( description contains 'SCP' )
```



(description contains 'SCP')

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
10/16 15:07:46	general	informational	general		File successfully uploaded after SCP transfer
10/16 15:07:44	general	informational	general		SCP import of panupv2-all-contents-8765-8342 type content by scp_admin user sucessfully completed

3. **Panorama** > 동적 업데이트를 선택하고 업로드한 콘텐츠 버전을 다운로드할 수 있는지 확인합니다.



Applications and Threats **Last checked:** 2023/10/16 14:51:45 PDT **Schedule:** Every Wednesday at 01:02 (Download only)

8756-8299	panupv2-all-contents-8756-8299.eap	Apps, Threats	Full	78 MB	1a317de34...	2023/09/19 11:19:45 PDT			Download
8763-8329	panupv2-all-contents-8763-8329	Apps, Threats	Full	78 MB	53c35ba39...	2023/10/05 23:41:22 PDT			Download
8763-8330	panupv2-all-contents-8763-8330	Apps, Threats	Full	78 MB	1ad100f1fa...	2023/10/06 15:02:41 PDT			Download
8763-8331	panupv2-all-contents-8763-8331.eap	Apps, Threats	Full	79 MB	2a64e53c1...	2023/10/06 16:10:58 PDT			Download
8763-8332	panupv2-all-contents-8763-8332	Apps, Threats	Full	78 MB	a3f4385c59...	2023/10/06 20:44:58 PDT			Download
8763-8333	panupv2-all-contents-8763-8333	Apps, Threats	Full	78 MB	f374b9126...	2023/10/09 19:16:46 PDT			Download
8763-8334	panupv2-all-contents-8763-8334.eap	Apps, Threats	Full	79 MB	901d16c05...	2023/10/09 20:12:57 PDT	✓		Install Review Policie Review Apps
8764-8335	panupv2-all-contents-8764-8335	Apps, Threats	Full	78 MB	1b5b7cad7...	2023/10/11 17:12:22 PDT			Download
8764-8336	panupv2-all-contents-8764-8336.eap	Apps, Threats	Full	79 MB	8ad97ff175...	2023/10/11 17:39:31 PDT			Download
8765-8338	panupv2-all-contents-8765-8338	Apps, Threats	Full	78 MB	8718ecb41...	2023/10/13 09:54:19 PDT			Download
8765-8339	panupv2-all-contents-8765-8339	Apps, Threats	Full	78 MB	aecf670c1c...	2023/10/13 17:36:39 PDT			Download
8765-8340	panupv2-all-contents-8765-8340.eap	Apps, Threats	Full	79 MB	f916e0f452...	2023/10/13 21:11:46 PDT			Download
8765-8341	panupv2-all-contents-8765-8341	Apps, Threats	Full	79 MB	6740f7c0f5...	2023/10/13 21:26:49 PDT			Download
8765-8342	panupv2-all-contents-8765-8342	Apps, Threats	Full	78 MB	4eb481c89...	2023/10/16 12:07:56 PDT			Download Review Policie Review Apps
8765-8343	panupv2-all-contents-8765-8343.eap	Apps, Threats	Full	79 MB	21562c493...	2023/10/16 12:17:48 PDT			Download

관리자 활동 추적 구성

Panorama™ 관리 서버, 관리 방화벽 및 로그 수집기의 웹 인터페이스 및 CLI에서 관리자 활동을 추적하여 배포 전반의 활동을 실시간으로 보고합니다. 관리자 계정이 손상되었다고 믿을 만한 이유가 있는 경우 이 관리자 계정이 웹 인터페이스 전체에서 탐색한 위치 또는 그들이 실행한 운영 명령에 대한 전체 기록이 있으므로 세부적으로 분석하고 손상된 관리자가 취한 모든 조치에 대응할 수 있습니다.

이벤트가 발생하면 관리자가 웹 인터페이스를 탐색하거나 CLI에서 운영 명령이 실행될 때마다 감사 로그가 생성되어 지정된 syslog 서버로 포워딩됩니다. 실행된 각 탐색 또는 추천에 대해 감사 로그가 생성됩니다. 예를 들어 새 주소 개체를 생성하려는 경우를 생각해 보십시오. 개체를 클릭하면 감사 로그가 생성되고 주소를 클릭하면 두 번째 감사 로그가 생성됩니다.

감사 로그는 syslog 서버로 포워딩된 syslog로만 볼 수 있으며 Panorama 또는 관리되는 방화벽 웹 인터페이스에서는 볼 수 없습니다. 감사 로그는 syslog 서버로만 포워딩할 수 있고 Strata Logging Service로는 포워딩할 수 없으며 방화벽, Panorama 또는 로그 수집기에 로컬로 저장되지 않습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama, 관리 방화벽 및 로그 수집기에 대한 관리자 활동의 감사 로그를 포워딩하도록 syslog 서버 프로파일을 구성합니다.

이 단계는 관리자 활동 추적을 위한 감사 로그를 성공적으로 저장하는 데 필요합니다.

1. **Panorama** > 서버 프로파일 > **Syslog**를 선택한 다음 새 syslog 서버 프로파일을 추가합니다.
2. syslog 서버 프로파일을 구성합니다.

STEP 2 | 관리 방화벽에 대한 관리자 활동 추적을 구성합니다.

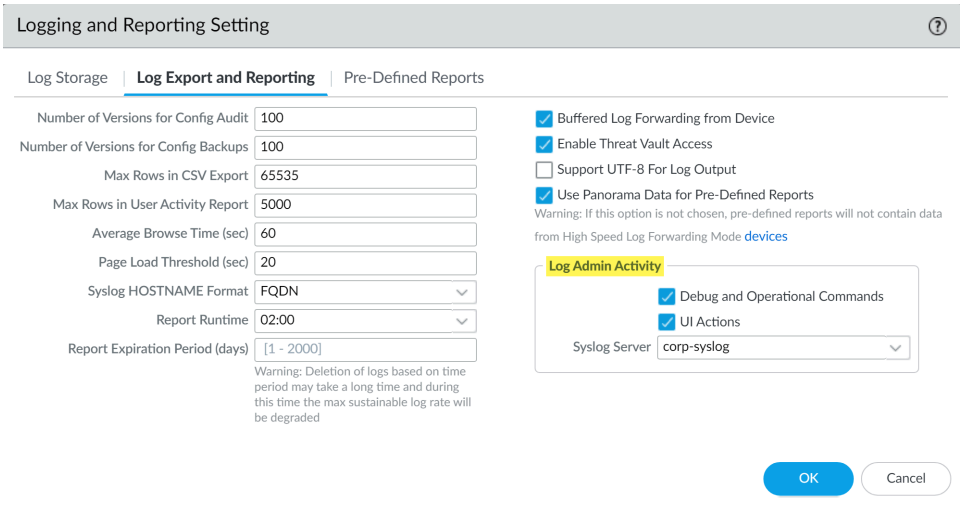
이 단계는 관리 방화벽에서 관리자 활동을 추적하기 위한 감사 로그를 성공적으로 저장하는 데 필요합니다.

1. 디바이스 > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
2. 관리자 활동 추적을 구성합니다.
3. 커밋 및 커밋 및 푸시를 선택합니다.

STEP 3 | Panorama에 대한 관리자 활동 추적을 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
2. 로그 내보내기 및 보고를 선택합니다.
3. 관리자 활동 기록 섹션에서 추적할 관리자 활동을 구성합니다.
   - 작동 명령 - 관리자가 CLI에서 작동 또는 디버그 명령을 실행하거나 웹 인터페이스에서 트리거된 작동 명령을 실행할 때 감사 로그를 생성합니다. PAN-OS 작동 및 디버그 명령의 전체 목록은 CLI 작동 명령 레이어를 참조하십시오.
   - **UI** 작업 - 관리자가 웹 인터페이스 전체를 탐색할 때 감사 로그를 생성합니다. 여기에는 구성 탭 간 탐색과 탭 내의 개별 개체가 포함됩니다.

     예를 들어, 관리자가 **ACC**에서 정책 탭으로 이동할 때 감사 로그가 생성됩니다. 또한 관리자가 **Objects** > **Addresses**에서 **Objects** > **Tags**로 이동할 때 감사 로그가 생성됩니다.
   - **Syslog** 서버 - 감사 로그를 포워딩할 대상 syslog 서버 프로파일을 선택합니다.
4. 확인을 클릭합니다.



5. 커밋 및 **Panorama**에 커밋을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 수집기 그룹의 로그 수집기에 대한 관리자 활동 추적을 구성합니다.

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 클릭합니다.
2. 감사를 선택합니다.
3. Log Admin Activity 섹션에서 CLI 활동에 대한 감사 추적을 구성합니다.

   로그 수집기는 *CLI*를 통해서만 로그 수집기에 액세스할 수 있으므로 로그 수집기에 대한 *CLI* 활동만 추적할 수 있습니다.

   - 작동 명령 - 관리자가 CLI에서 작동 또는 디버그 명령을 실행할 때 감사 로그를 생성합니다. PAN-OS 작동 및 디버그 명령의 전체 목록은 CLI 작동 명령 계층을 참조하십시오.
   - **Syslog** 서버 - 감사 로그를 포워딩할 대상 syslog 서버 프로파일을 선택합니다.
4. 확인을 클릭합니다.
5. 커밋 및 **Panorama**에 커밋을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

사용자 지정 인증서를 사용하여 인증 설정

기본적으로 Palo Alto Networks 디바이스는 상호 인증을 위해 사전 정의된 인증서를 사용하여 관리 액세스 및 디바이스 간 통신에 사용되는 SSL 연결을 설정합니다. 그러나 대신 사용자 지정 인증서를 사용하여 인증을 구성할 수 있습니다. 또한 사용자 지정 인증서를 사용하여 Panorama HA 피어 간의 고가용성(HA) 연결을 보호할 수 있습니다. 사용자 지정 인증서를 사용하면 Panorama와 관리되는 방화벽 및 로그 수집기 간의 상호 인증을 보장하기 위해 고유한 신뢰 체인을 설정할 수 있습니다. 인증서와 Panorama, Log Collectors 및 방화벽에 인증서를 배포하는 방법에 대한 자세한 내용은 인증서 관리를 참조하십시오.

다음 주제에서는 Panorama를 사용하여 사용자 지정 인증서를 구성하고 관리하는 방법을 설명합니다.

- SSL/TLS 연결은 어떻게 상호 인증됩니까?
- Panorama에서 사용자 지정 인증서를 사용하여 인증 구성
- 관리되는 디바이스에서 사용자 지정 인증서를 사용하여 인증 구성
- 새 클라이언트 디바이스 추가
- 인증서 변경

SSL/TLS 연결은 어떻게 상호 인증됩니까?

일반 SSL 연결에서는 서버만 인증서를 제시하여 클라이언트에게 자신을 식별하면 됩니다. 그러나 상호 SSL 인증에서 클라이언트는 서버에도 인증서를 제공합니다. Panorama, 기본 Panorama HA 피어, 로그 수집기, WildFire 어플라이언스 및 PAN-DB 어플라이언스가 서버 역할을 할 수 있습니다. 방화벽, 로그 수집기, WildFire 어플라이언스 및 보조 Panorama HA 피어가 클라이언트 역할을 할 수 있습니다. 디바이스가 수행하는 역할은 배포에 따라 다릅니다. 예를 들어 아래 다이어그램에서 Panorama는 여러 방화벽과 수집기 그룹을 관리하고 방화벽 및 로그 수집기의 서버 역할을 합니다. Log Collector는 로그를 보내는 방화벽에 대한 서버 역할을 합니다.

배포에서 상호 인증을 위한 사용자 지정 인증서를 배포하려면 다음이 필요합니다.

- **SSL/TLS** 서비스 프로파일 - SSL/TLS 서비스 프로파일은 사용자 지정 인증서를 참조하고 서버 디바이스가 클라이언트 디바이스와 통신하는 데 사용하는 SSL/TLS 프로토콜 버전을 설정하여 연결 보안을 정의합니다.
- 서버 인증서 및 프로파일 - 서버 역할의 디바이스는 클라이언트 디바이스에서 자신을 식별하기 위해 인증서와 인증서 프로파일이 필요합니다. 엔터프라이즈 PKI(공개 키 인프라)에서 이 인증서를 배포하거나, 신뢰할 수 있는 타사 CA에서 구매하거나, 로컬에서 자체 서명된 인증서를 생성할 수 있습니다. 서버 인증서는 인증서 일반 이름(CN) 또는 주체 대체 이름에 디바이스 관리 인터페이스의 IP 주소 또는 FQDN을 포함해야 합니다. 클라이언트 방화벽 또는 로그 수집기는 서버의 ID를 확인하기 위해 서버의 IP 주소 또는 FQDN에 대해 서버가 제시하는 인증서의 CN 또는 주체 대체 이름을 일치시킵니다.

  또한 인증서 프로파일을 사용하여 인증서 해지 상태(OCSP/CRL)와 해지 상태에 따라 수행되는 작업을 정의합니다.
- 클라이언트 인증서 및 프로파일 - 관리되는 각 디바이스에는 클라이언트 인증서와 인증서 프로파일이 필요합니다. 클라이언트 디바이스는 인증서를 사용하여 서버 디바이스에 자신을 식별합니다. SCEP(단

 ©2024 Palo Alto Networks, Inc.

순 인증서 등록 프로토콜)를 사용하여 엔터프라이즈 PKI에서 인증서를 배포하거나, 신뢰할 수 있는 타사 CA에서 인증서를 구매하거나, 로컬에서 자체 서명된 인증서를 생성할 수 있습니다.

사용자 지정 인증서는 각 클라이언트 디바이스에 고유하거나 모든 디바이스에 공통적일 수 있습니다. 고유한 디바이스 인증서는 관리되는 디바이스 및 CN의 일련번호 해시를 사용합니다. 서버는 CN 또는 주체 대체 이름을 클라이언트 디바이스의 구성된 일련번호와 일치시킵니다. CN을 기반으로 하는 클라이언트 인증서 유효성 검사가 발생하려면 사용자 이름을 주체 공통 이름으로 설정해야 합니다. 클라이언트 인증서 동작은 Panorama HA 피어 연결에도 적용됩니다.

각 클라이언트 디바이스에서 클라이언트 인증서 및 인증서 프로파일을 구성하거나 템플릿의 일부로 Panorama에서 각 디바이스로 구성을 푸시할 수 있습니다.

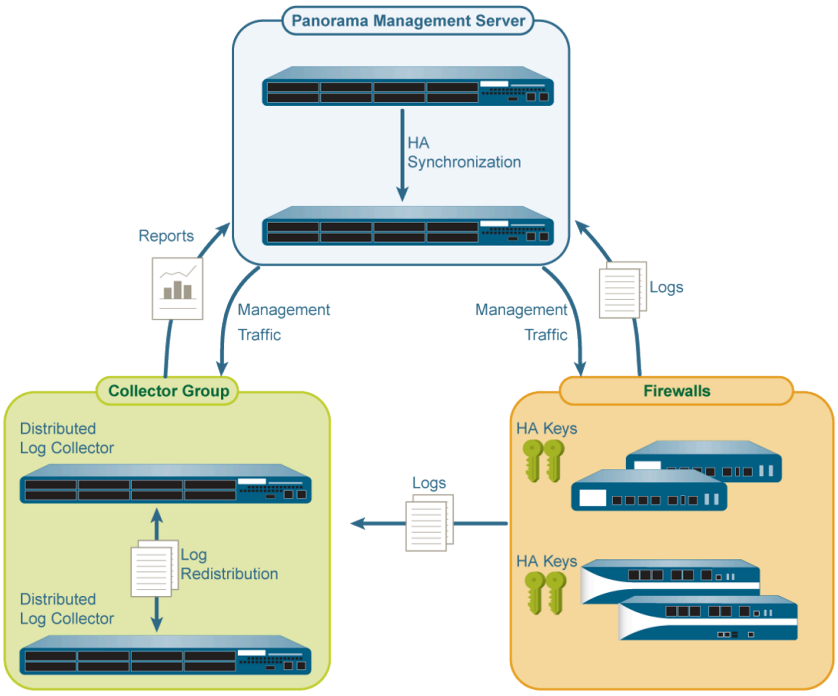


그림 **10: SSL/TLS** 인증

Panorama에서 사용자 지정 인증서를 사용하여 인증 구성

배포에서 관리되는 디바이스와의 상호 인증을 위해 사전 정의된 인증서 대신 사용자 지정 인증서를 사용하도록 서버 사이드(Panorama)를 구성하려면 다음 절차를 완료하십시오. Panorama HA 쌍에서 사용자 지정 인증서를 구성하려면 HA 피어 간에 사용자 지정 인증서를 사용하여 인증 설정을(를) 참조하십시오.

STEP 1 | 서버 인증서를 배포합니다.

Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA(인증 기관) 또는 신뢰할 수 있는 타사 CA에서 인증서를 가져와 Panorama 또는 서버 Log Collector에 인증서를 배포할 수 있습니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에서 인증서 프로파일 구성 이 인증서 프로파일은 사용할 인증서와 IP 주소 또는 FQDN을 찾을 인증서 필드를 정의합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

   인증서 프로파일의 일부로 중간 *CA*를 구성하는 경우 루트 *CA*도 포함해야 합니다.

STEP 3 | SSL/TLS 서비스 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. Panorama 및 해당 관리 디바이스가 SSL/TLS 서비스에 사용하는 인증서 및 프로토콜을 정의하도록 SSL/TLS 프로파일을 구성합니다.

STEP 4 | 서버 역할의 Panorama 또는 Log Collector에서 보안 서버 통신을 구성합니다.

1. 다음 탐색 경로 중 하나를 선택합니다.
   - Panorama: **Panorama** > 설정통신 보안 설정 > 관리 및 편집
   - 로그 수집기의 경우: **Panorama** > **Managed Collectors** > 통신 > 추가
2. 사용자 지정 보안 서버 통신 옵션을 선택합니다.
3. 사용자 지정 인증서만 허용 확인란이 선택되어 있지 않은지 확인합니다. 이를 통해 사용자 지정 인증서로 마이그레이션하는 동안 모든 디바이스를 계속 관리할 수 있습니다.

   사용자 지정 인증서만 확인란을 선택하면 *Panorama*는 사전 정의된 인증서를 사용하여 디바이스를 인증하지 않고 관리할 수 없습니다.
4. **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 Panorama, 방화벽, 로그 수집기 및 Panorama HA 피어 간의 모든 SSL 연결에 적용됩니다.
5. 방화벽과 같은 클라이언트와의 통신 보안을 설정하는 데 사용할 인증서를 식별하는 인증서 프로파일을 선택합니다.
6. (선택 사항) 권한 부여 목록을 구성합니다. 권한 부여 목록은 인증서 인증 이상의 보안 계층을 추가합니다. 인증 목록은 클라이언트 인증서 주체 또는 주체 대체 이름을 확인합니다. 클라이언트

 ©2024 Palo Alto Networks, Inc.

인증서와 함께 제공된 주체 또는 주체 대체 이름이 인증 목록의 식별자와 일치하지 않으면 인증이 거부됩니다.

일련번호를 기반으로 클라이언트 디바이스를 인증할 수도 있습니다.

1. 권한 부여 목록을 추가합니다.
2. 인증서 프로파일에 구성된 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
3. 식별자가 제목인 경우 일반 이름을 입력하고 식별자가 제목 대체 이름인 경우 IP 주소, 호스트 이름 또는 이메일을 입력합니다.
4. 확인을 클릭합니다.
5. 권한 부여 목록 확인을 선택하여 권한 부여 목록을 시행하십시오.

7. 서버가 관리 디바이스의 일련번호를 기반으로 클라이언트를 인증 하도록 하려면 일련번호를 기반으로 클라이언트 인증을 선택합니다. 이 유형의 인증을 사용하려면 클라이언트 인증서의 CN 또는 주체에 특수 키워드 $UDID가 있어야 합니다.
8. 사용자 지정 인증서를 사용하여 데이터 재배포 클라이언트와의 나가는 통신을 보호하려면 통신 사용자 지정 섹션에서 데이터 재배포 옵션을 선택합니다.
9. 연결 해제 대기 시간(분)에서 현재 세션을 종료하고 관리되는 디바이스와의 연결을 다시 설정하기 전에 Panorama가 기다려야 하는 시간을 지정합니다. 이 필드는 기본적으로 비어 있으며 범위는 0~44,640분입니다. 이 필드를 비워 두는 것은 0으로 설정하는 것과 같습니다.

   연결 해제 대기 시간은 새 구성을 커밋할 때까지 카운트다운을 시작하지 않습니다.

10. 확인을 클릭합니다.
11. 변경 사항을 커밋합니다.

관리되는 디바이스에서 사용자 지정 인증서를 사용하여 인증 구성

배포에서 관리되는 디바이스와의 상호 인증을 위해 사전 정의된 인증서 대신 사용자 지정 인증서를 사용하도록 클라이언트 측(방화벽 또는 로그 수집기)을 구성하려면 다음 절차를 완료하십시오.

STEP 1 | 각 관리되는 방화벽 또는 로그 수집기를 업그레이드합니다. 사용자 지정 인증서 인증을 시행하려면 모든 관리 디바이스에서 PAN-OS 8.0 이상의 버전을 실행해야 합니다.

방화벽을 업그레이드하십시오. 업그레이드 후 각 방화벽은 사전 정의된 기본 인증서를 사용하여 Panorama에 연결합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 디바이스 인증서를 얻거나 생성합니다.

Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA(인증 기관) 또는 신뢰할 수 있는 타사 CA에서 인증서를 가져와 Panorama 또는 서버 Log Collector에 인증서를 배포할 수 있습니다.

일련번호를 기반으로 클라이언트 디바이스를 인증하는 경우 일반 이름을 $UDID로 설정하거나 CN=$UDID(SCEP 프로파일에서)를 따릅니다.

- Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA 또는 신뢰할 수 있는 타사 CA에서 인증서를 얻을 수 있습니다.
- 디바이스 인증서에 SCEP를 사용하는 경우 SCEP 프로파일을 구성합니다. SCEP를 사용하면 관리되는 디바이스에 인증서를 자동으로 배포할 수 있습니다. SCEP 프로파일이 있는 새 클라이언트 디바이스가 Panorama로 인증을 시도하면 인증서가 SCEP 서버에서 디바이스로 전송됩니다.

STEP 3 | 클라이언트 디바이스에 대한 인증서 프로파일을 구성합니다.

각 클라이언트 디바이스에서 개별적으로 구성하거나 템플릿의 일부로 이 구성을 관리 디바이스에 푸시할 수 있습니다.

1. 다음 탐색 경로 중 하나를 선택합니다.
   - 방화벽의 경우 디바이스 > 인증서 관리 > 인증서 프로파일을 선택합니다.
   - 로그 수집기의 경우 - **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

STEP 4 | 각 방화벽 또는 로그 수집기에 사용자 지정 인증서를 배포합니다.

1. 다음 탐색 경로 중 하나를 선택합니다.
   - 방화벽의 경우: 디바이스 > 설정 > 관리를 선택하고 Panorama 설정 편집
   - 로그 수집기의 경우: **Panorama** > **Managed Collectors**를 선택하고 새 로그 수집기를 추가하거나 기존 수집기를 선택합니다. 통신을 선택합니다.
2. 보안 클라이언트 통신 확인란을 선택합니다(방화벽만 해당).
3. 인증서 유형을 선택합니다.
   - 로컬 디바이스 인증서를 사용하는 경우 인증서 및 인증서 프로파일을 선택합니다.
   - SCEP를 사용하여 디바이스 인증서를 배포하는 경우 **SCEP** 프로파일 및 인증서 프로파일을 선택합니다.
   - 기본 Panorama 인증서를 사용하는 경우 사전 정의를 선택합니다.
4. (선택 사항) 서버 **ID** 확인을 활성화합니다. 방화벽 또는 로그 수집기는 서버 인증서의 CN을 Panorama의 IP 주소 또는 FQDN과 비교하여 ID를 확인합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

   변경 사항을 커밋한 후 관리 디바이스는 연결 해제 대기 시간이 완료될 때까지 Panorama와의 현재 세션을 종료하지 않습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 사용자 지정 인증서를 사용하려는 수신 통신 유형을 선택합니다.

- **HA** 커뮤니케이션
- **WildFire Communication**
- 데이터 재배포

STEP 6 | 모든 관리 디바이스에 사용자 지정 인증서를 배포한 후 사용자 지정 인증서를 사용하여 인증을 시행합니다.

> *WildFire* 어플라이언스는 현재 사용자 지정 인증서를 지원하지 않습니다. *Panorama*가 *WildFire* 어플라이언스를 관리하는 경우 사용자 지정 인증서만 허용을 선택하지 마십시오.

1. **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.
2. 사용자 지정 인증서만 허용을 선택합니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

   이 변경 사항을 커밋한 후 Panorama에서 관리하는 모든 디바이스는 사용자 지정 인증서를 사용해야 합니다. 그렇지 않으면 Panorama와 디바이스 간의 인증이 실패합니다.

새 클라이언트 디바이스 추가

새 방화벽이나 Log Collector를 Panorama에 추가할 때 워크플로는 이러한 디바이스가 상호 인증에만 사용자 지정 인증서를 사용하도록 구성되었는지의 여부에 따라 다릅니다.

- Panorama에서 Custom Certificates Only를 선택하지 않은 경우 Panorama에 디바이스를 추가한 다음 관리되는 디바이스에서 사용자 지정 인증서를 사용하여 인증 구성 단계에서 시작하는 프로세스에 따라 사용자 지정 인증서를 배포할 수 있습니다.
- Panorama에서 Custom Certificates Only를 선택한 경우 Panorama에 추가하기 전에 방화벽에 사용자 지정 인증서를 배포해야 합니다. 그렇지 않은 경우 관리되는 디바이스는 Panorama로 인증할 수 없습니다. 이것은 방화벽 웹 인터페이스를 통해 또는 bootstrap.xml 파일의 일부로 부트스트랩을 통해 수동으로 수행할 수 있습니다.

인증서 변경

배포의 사용자 지정 인증서가 만료되었거나 취소되어 교체해야 하는 경우 아래 작업 중 하나를 완료할 수 있습니다.

- 서버 인증서 변경
- 클라이언트 인증서 변경
- 루트 또는 중간 CA 인증서 변경

서버 인증서 변경

서버 인증서를 교체하려면 다음 작업을 완료하십시오.

©2024 Palo Alto Networks, Inc.

STEP 1 | 새 서버 인증서를 배포합니다.

Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA 또는 신뢰할 수 있는 타사 CA에서 인증서를 가져와 Panorama 또는 서버 Log Collector에 인증서를 배포할 수 있습니다.

STEP 2 | SSL/TLS 서비스 프로파일에서 인증서를 변경합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택하고 SSL/TLS 서비스 프로파일을 선택합니다.
2. 인증서를 선택합니다.
3. 확인을 클릭합니다.

STEP 3 | 서버(Panorama 또는 로그 수집기)와 클라이언트 디바이스 간의 연결을 다시 설정합니다.

1. **Panorama** > 설정 > 관리를 선택하고 Panorama에 대한 Panorama 설정을 편집하거나 **Panorama** > 관리 수집기 > 로그 수집기에 대한 > 통신 추가를 선택합니다.
2. 연결 해제 대기 시간을 설정합니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

클라이언트 인증서 변경

클라이언트 인증서를 교체하려면 다음 작업을 완료하십시오.

STEP 1 | 디바이스 인증서를 얻거나 생성합니다.

Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA 또는 신뢰할 수 있는 타사 CA에서 인증서를 가져와 Panorama 또는 서버 Log Collector에 인증서를 배포할 수 있습니다.

일련번호를 기반으로 클라이언트 디바이스를 인증하는 경우 일반 이름을 $UDID로 설정하거나 CN=$UDID(SCEP 프로파일에서)를 따릅니다.

- Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA 또는 신뢰할 수 있는 타사 CA에서 인증서를 얻을 수 있습니다.
- 디바이스 인증서에 SCEP를 사용하는 경우 SCEP 프로파일을 구성합니다. SCEP를 사용하면 관리되는 디바이스에 인증서를 자동으로 배포할 수 있습니다. SCEP 프로파일이 있는 새 클라이언트 디바이스가 Panorama로 인증을 시도하면 인증서가 SCEP 서버에서 디바이스로 전송됩니다.

STEP 2 | 인증서 프로파일에서 인증서를 변경합니다.

1. 디바이스 > 인증서 관리 > 인증서 프로파일을 선택하고 인증서 프로파일을 선택합니다.
2. CA 인증서 아래에서 인증서 프로파일에 할당할 새 인증서를 추가합니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

루트 또는 중간 CA 인증서 변경

루트 또는 중간 CA 인증서를 교체하려면 다음 작업을 완료하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 클라이언트에서 사전 정의된 인증서를 수락하도록 서버를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.
2. 사용자 지정 인증서만 선택을 취소합니다.
3. 인증서 프로파일 드롭다운에서 없음을 선택합니다.
4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

STEP 2 | 새 루트 또는 중간 CA 인증서를 배포합니다.

Panorama에서 자체 서명된 인증서를 생성하거나 엔터프라이즈 CA 또는 신뢰할 수 있는 타사 CA에서 인증서를 가져와 Panorama 또는 서버 Log Collector에 인증서를 배포할 수 있습니다.

STEP 3 | 서버 인증서 프로파일에서 CA 인증서를 업데이트합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택하고 업데이트할 인증서 프로파일을 선택합니다.
2. 이전 CA 인증서를 삭제합니다.
3. 새 CA 인증서를 추가합니다.
4. 확인을 클릭합니다.

STEP 4 | 새 클라이언트 인증서를 생성하거나 가져옵니다.

1. 디바이스 > 인증서 관리 > 인증서를 선택합니다.
2. 자체 서명된 루트 CA 인증서를 생성하거나 엔터프라이즈 CA에서 인증서를 가져옵니다.

STEP 5 | 클라이언트 인증서 프로파일에서 CA 인증서를 업데이트합니다.

1. 디바이스 > 설정 > 관리를 선택하고 방화벽의 경우 Panorama 설정에서 편집 아이콘을 클릭하거나, **Panorama** > 관리형 수집기 > 통신 > 추가를 선택하고 업데이트할 인증서 프로파일을 선택합니다.
2. 이전 CA 인증서를 삭제합니다.
3. 새 CA 인증서를 추가합니다.
4. 확인을 클릭합니다.

STEP 6 | 모든 관리 디바이스에서 CA 인증서를 업데이트한 후 사용자 지정 인증서 인증을 시행하십시오.

1. **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.
2. 사용자 지정 인증서만을 선택합니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

   이 변경 사항을 커밋한 후 Panorama에서 관리하는 모든 디바이스는 사용자 지정 인증서를 사용해야 합니다. 그렇지 않으면 Panorama와 디바이스 간의 인증이 실패합니다.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

방화벽 관리

Palo Alto Networks 방화벽을 관리하기 위해 Panorama™ 관리 서버를 사용하려면 방화벽을 관리 디바이스로 추가한 다음 디바이스 그룹과 템플릿 또는 템플릿 스택(template stack)에 할당해야 합니다. 다음 작업은 최초 방화벽 배포에 가장 적합합니다. 계속하기 전에 Panorama 배포 계획을 검토하여 배포 옵션을 이해하십시오.

- 관리되는 디바이스로 방화벽 추가
- 관리 방화벽에 대한 디바이스 인증서 설치
- Panorama 관리와 클라우드 관리 간의 변경 사항
- 제로 터치 프로비저닝 설정
- 디바이스 그룹 관리
- 템플릿 및 템플릿 스택(template stack) 관리
- Panorama에서 마스터 키 관리
- 관리되는 방화벽에 대한 구성 푸시 예약
- 관리되는 방화벽에 데이터 재분배
- 방화벽을 Panorama 관리로 전환
- Panorama 디바이스 모니터링
- 사용 사례: Panorama를 사용하여 방화벽 구성

Panorama 웹 인터페이스에서 개체 및 정책 탭을 보려면 먼저 하나 이상의 디바이스 그룹을 생성해야 합니다. 네트워크 및 디바이스 탭을 보려면 템플릿을 하나 이상 생성해야 합니다. 이러한 탭에는 네트워크에서 방화벽을 구성하고 관리하는 옵션이 포함되어 있습니다.

관리되는 디바이스로 방화벽 추가

Panorama™ 관리 서버를 사용하여 방화벽을 관리하려면 방화벽과 Panorama 관리 서버 간의 연결을 활성화해야 합니다. 새 방화벽을 온보딩할 때 보안 태세를 강화하려면 새 방화벽과 처음 연결할 때 서버 간의 상호 인증을 위해 Panorama 관리 서버에 고유한 디바이스 등록 인증 키를 생성해야 합니다. 성공적인 첫 번째 연결을 위해서는 서버가 관리할 각 방화벽에 Panorama IP 주소를 추가하고, 각 방화벽에 대해 서버에 일련번호를 추가하고, 서버와 방화벽 모두에서 디바이스 등록 인증 키를 지정해야 합니다. 방화벽을 관리되는 디바이스로 추가하면 초기 배포 중에 새 방화벽을 디바이스 그룹, 템플릿 스택(template stack), 수집기 그룹 및 로그 수집기와 연결할 수도 있습니다. 또한 방화벽이 Panorama 서버에 처음 연결될 때 새로 추가된 방화벽에 구성을 자동으로 푸시하는 옵션이 있어 방화벽이 즉시 구성되고 네트워크를 보호할 준비가 됩니다.

고가용성(HA) 구성에서 방화벽을 Panorama에 추가하는 경우, 디바이스 등록 인증 키는 기본 피어에 방화벽을 추가하는 데만 필요합니다. HA 구성의 Panorama는 HA 장애 조치 시 보조 피어가 방화벽을 관리할 수 있도록 하는 CA(인증 기관) 인증서를 동기화합니다.

방화벽을 관리형 디바이스로 추가하려면 관리형 방화벽의 총 개수가 *Panorama*에서 활성화된 디바이스 관리 라이선스를 초과하지 않아야 합니다. ***Panorama*** > 라이선스를 선택하여 *Panorama*에서 활성화된 *#### ## ####*와 지원되는 관리형 방화벽의 최대 개수를 확인합니다.

추가하려는 방화벽이 디바이스 관리 라이선스 제한을 초과하면 작업이 차단되고 *Panorama* 관리에 방화벽을 추가하지 못했다는 경고 메시지가 표시됩니다.

방화벽은 서버 등록을 위해 Panorama 관리 서버 IP 주소를 사용합니다. Panorama 서버와 방화벽은 구성 관리 및 로그 수집을 위해 2,048비트 인증서와 AES-256 암호화 SSL 연결을 사용하여 서로 인증합니다.

디바이스 등록 인증 키를 구성하려면 키 수명과 인증 키를 사용하여 새 방화벽을 온보딩할 수 있는 횟수를 지정합니다. 또한 인증 키가 유효한 방화벽 일련번호를 하나 이상 지정할 수 있습니다. 방화벽이 Panorama에서 생성한 인증 키를 사용할 때마다 시스템 로그가 생성됩니다. 방화벽은 이후의 모든 통신에 사용되는 디바이스 인증서를 전달할 때 인증 키를 사용하여 Panorama 서버를 인증합니다.

PAN-OS 11.0.0 이상 릴리즈를 실행하는 *Panorama*는 *PAN-OS 10.1.3* 이상 릴리즈만 실행하는 온보딩 방화벽을 지원합니다. *Panorama*가 *PAN-OS 11.0*을 실행 중인 경우 *PAN-OS 10.1.2* 또는 *PAN-OS 10.1* 이전 릴리즈를 실행하는 방화벽을 *Panorama* 관리에 추가할 수 없습니다.

*Panorama*는 다음 릴리스를 실행하는 온보딩 방화벽을 지원합니다.

- ***PAN-OS 11.0.0*** 이상 릴리즈를 실행하는 ***Panorama*** — *PAN-OS 10.1.3* 이상 릴리즈를 실행하는 방화벽 및 *PAN-OS 10.0* 또는 *PAN-OS* 이전 릴리즈를 실행하는 방화벽.

*PAN-OS 10.2*로 업그레이드할 때 *Panorama*에서 이미 관리 중인 방화벽에는 영향이 없습니다.

Panorama 관리에 방화벽을 추가하는 데 문제가 발생한 경우 Panorama에 대해 관리되는 디바이스 연결을 복구해야 할 수 있습니다.

©2024 Palo Alto Networks, Inc.

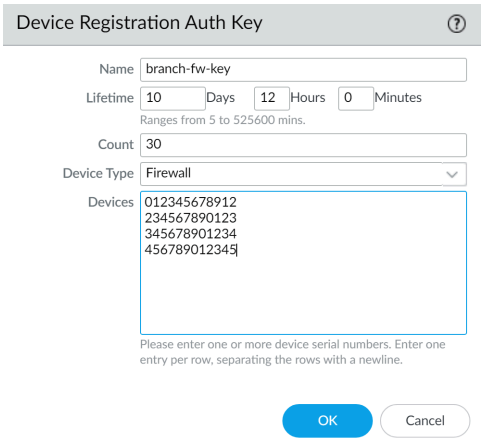
STEP 1 | 방화벽을 설정합니다.

1. 방화벽에 액세스할 수 있고 네트워크를 통해 Panorama 서버와 통신할 수 있도록 초기 구성을 수행합니다.
2. Panorama 서버에서 구성 설정 및 정책 규칙을 푸시할 수 있도록 방화벽에서 사용할 각 데이터 인터페이스를 구성하고 보안 영역에 연결합니다.

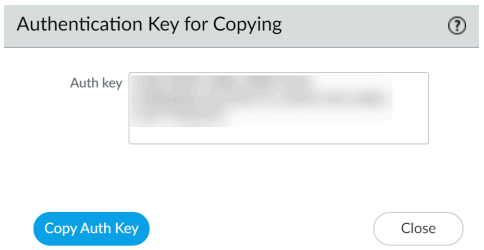
STEP 2 | 기기 등록 인증 키를 생성합니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
3. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 키 수명을 지정하여 인증 키를 사용하여 새 방화벽을 온보딩할 수 있는 기간을 제한합니다.
   - 개수 - 인증 키를 사용하여 새 방화벽을 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 방화벽만 인증하는 데 사용되도록 지정합니다.

     모두를 선택하여 디바이스 등록 인증 키를 사용하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 방화벽을 지정하기 위해 하나 이상의 디바이스 일련 번호를 입력합니다.
4. 확인을 클릭합니다.



5. 인증 키를 복사하고 닫습니다.

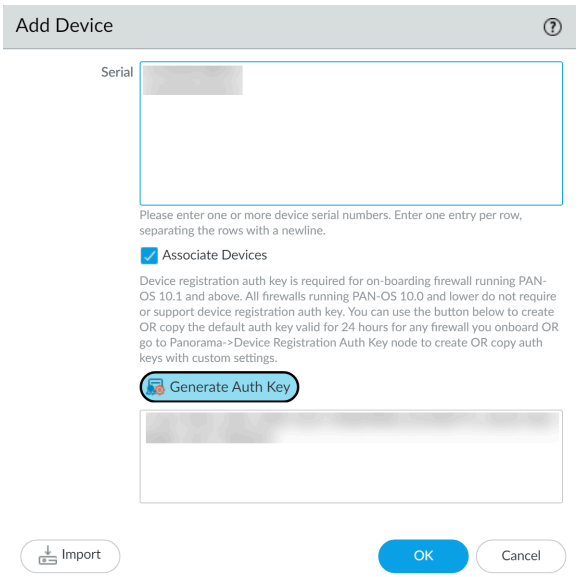


 ©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama 관리 서버에 방화벽을 추가합니다. CSV 파일을 사용하여 하나 이상의 방화벽을 수동으로 추가하거나 방화벽을 대량으로 가져올 수 있습니다.

단일 *vsys* 방화벽만 *Panorama* 관리 서버로 대량 가져올 수 있습니다. 둘 이상의 가상 시스템*(vsys)*이 있는 방화벽은 대량으로 가져올 수 없습니다.

- 하나 이상의 방화벽을 수동으로 추가합니다.
  1. **Panorama** > 관리되는 디바이스 > 요약를 선택하고 새 방화벽 추가를 선택합니다.
  2. 방화벽 일련번호를 입력합니다. 여러 방화벽을 추가하는 경우 별도의 줄에 각 일련 번호를 입력합니다.
  3. (선택 사항) 방화벽이 Panorama 관리 서버에 처음 연결할 때 방화벽을 디바이스 그룹, 템플릿 스택(template stack), 로그 수집기 또는 수집기 그룹과 연결하려면 디바이스 연결을 선택합니다.
  4. 생성한 기기 등록 인증 키를 입력합니다.



  5. 확인을 클릭합니다.
  6. 필요에 따라 관리 방화벽을 연결합니다.

     디바이스 연결을 선택하지 않은 경우 이 단계를 건너뛰고 계속해서 Panorama와 통신하도록 방화벽을 구성하십시오.

     1. 각 열의 드롭다운에서 필요에 따라 디바이스 그룹, 템플릿 스택**(template stack)**, 수집기 그룹 및 로그 수집기를 할당합니다.
     2. 첫 번째 연결 시 자동 푸시를 활성화하면 디바이스 그룹과 템플릿 스택(template stack) 구성이 Panorama 서버에 처음 연결될 때 새 디바이스에 자동으로 푸시됩니다.

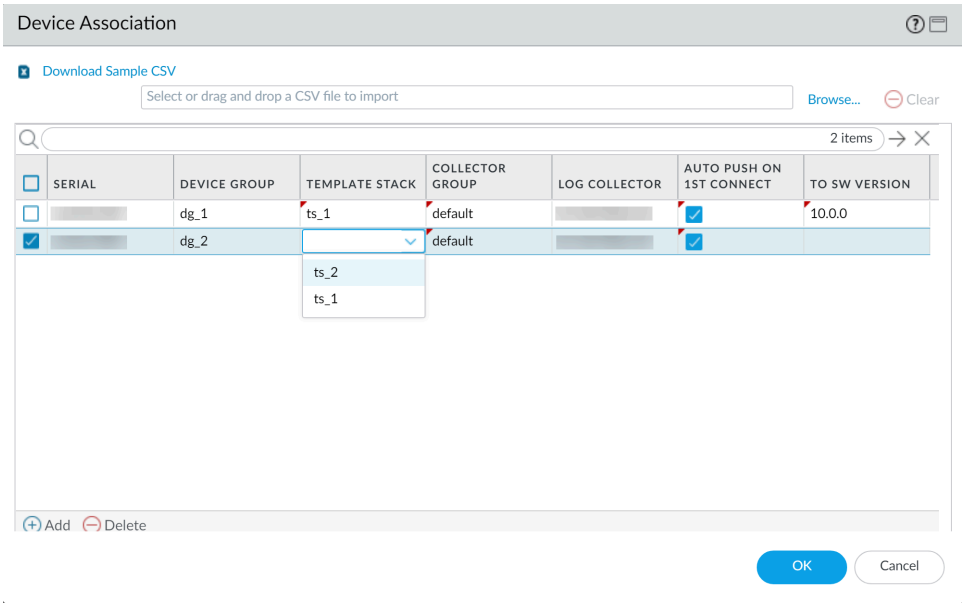
        첫 번째 연결 시 자동 푸시 옵션은 *PAN-OS® 8.1* 이상의 버전을 실행하는 방화벽에서만 지원됩니다. *## ## ##*은 *Panorama*에서 *PAN-OS 8.1* 이상의 버전을 실행하는 관리 디바이스로 실행됩니다.

©2024 Palo Alto Networks, Inc.

3. (선택 사항) Panorama 관리 서버에 성공적으로 연결되면 관리 방화벽을 지정된 PAN-OS 버전으로 자동 업그레이드를 시작하려면 PAN-OS 릴리스 버전(**SW** 버전으로 열)을 선택합니다.

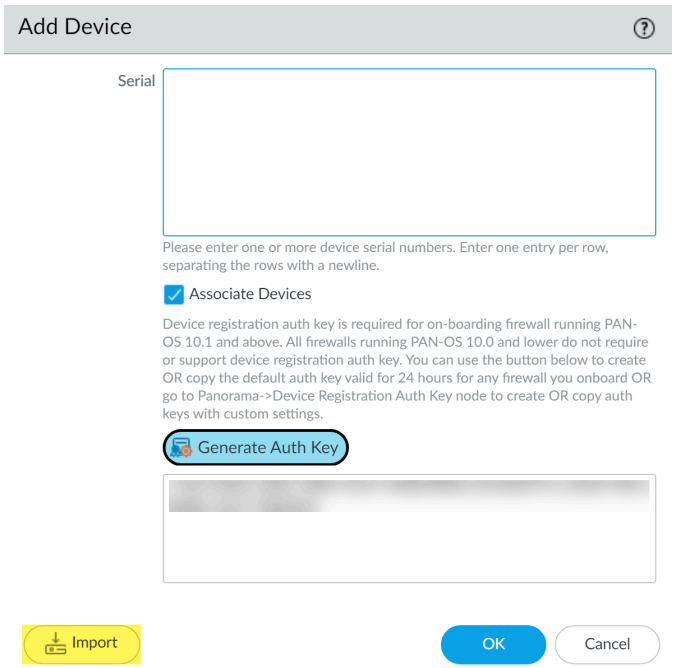
   관리 대상 방화벽을 처음 연결할 때 대상 *PAN-OS* 릴리스로 업그레이드하려면 방화벽을 관리 디바이스로 추가하기 전에 해당 *PAN-OS* 릴리스에 필요한 최소 콘텐츠 릴리스 버전을 설치해야 합니다. 이렇게 하려면 *Panorama* 관리에 방화벽을 추가하기 전에 방화벽을 등록하고 지원 라이선스를 활성화하고 콘텐츠 업데이트를 설치해야 합니다.

   관리 방화벽을 자동으로 업그레이드하지 않으려면 이 열을 비워 둡니다.
4. 확인을 클릭하여 디바이스를 추가합니다.



- CSV 파일을 사용하여 여러 방화벽을 대량으로 가져옵니다.
  1. **Panorama** > 관리되는 디바이스 > 요약을 선택하고 새 방화벽을 추가합니다.
  2. 생성한 기기 등록 인증 키를 추가합니다.
  3. 가져오기를 클릭합니다.

©2024 Palo Alto Networks, Inc.

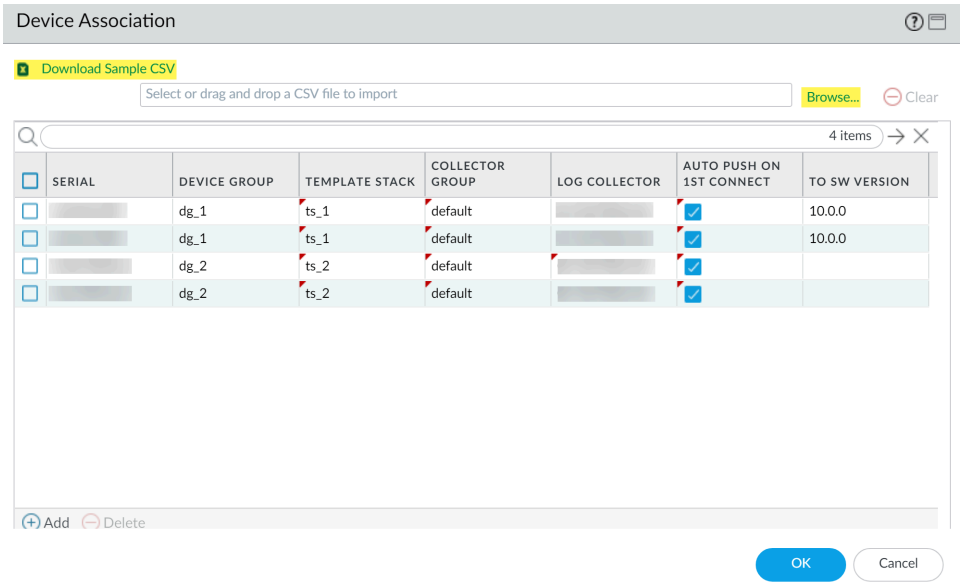


4. 샘플 **CSV**를 다운로드하고 다운로드한 CSV 파일을 추가하려는 방화벽으로 편집합니다. CSV에서 디바이스 그룹, 템플릿 스택(template stack), 수집기 그룹 및 로그 수집기에 방화벽을 할당하

 ©2024 Palo Alto Networks, Inc.

도록 선택하거나 방화벽 일련번호만 입력하고 웹 인터페이스에서 할당할 수 있습니다. 편집을 마친 후 CSV를 저장합니다.

5. 이전 단계에서 편집한 CSV 파일을 찾아 선택합니다.



6. CSV에 아직 할당되지 않은 경우 각 열의 드롭다운에서 필요에 따라 방화벽에 디바이스 그룹, 템플릿 스택, 수집기 그룹 및 로그 수집기를 할당합니다.
7. CSV에서 아직 활성화되지 않은 경우 첫 번째 연결 시 자동 푸시를 활성화하여 Panorama 서버에 처음 연결할 때 새 디바이스에 디바이스 그룹 및 템플릿 스택(template stack) 구성을 자동으로 푸시합니다.
8. (선택 사항) Panorama 서버에 성공적으로 연결되면 관리되는 방화벽을 지정된 PAN-OS 버전으로 자동 업그레이드를 시작하려면 PAN-OS 릴리스 버전(대상 **SW** 버전 열)을 선택합니다.

   관리 대상 방화벽을 처음 연결할 때 대상 *PAN-OS* 릴리스로 업그레이드하려면 방화벽을 관리 디바이스로 추가하기 전에 해당 *PAN-OS* 릴리스에 필요한 최소 콘텐츠 릴리스 버전을 설치해야 합니다. 이렇게 하려면 *Panorama* 관리에 방화벽을 추가하기 전에 방화벽을 등록하고 지원 라이선스를 활성화하고 콘텐츠 업데이트를 설치해야 합니다.

   관리 방화벽을 자동으로 업그레이드하지 않으려면 이 열을 비워 둡니다.
9. 확인을 클릭하여 방화벽을 추가합니다.

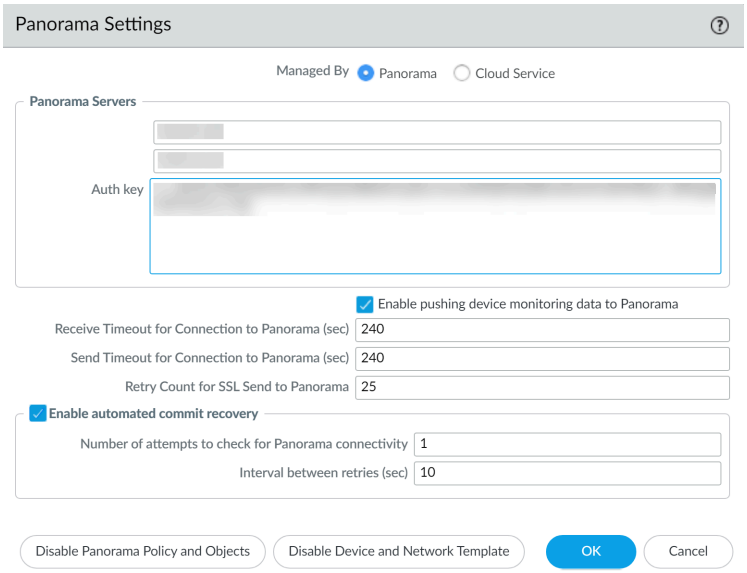
©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama 관리 서버와 통신하도록 방화벽을 구성합니다.

Panorama 서버가 관리할 각 방화벽에 대해 이 단계를 반복합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 방화벽에 대한 Panorama 설정을 구성합니다.
   1. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
   2. 관리자에서 **Panorama**를 선택합니다.
   3. 첫 번째 필드에 Panorama IP 주소를 입력합니다.

      *Panorama*는 디바이스 관리, 로그 수집, 보고 및 동적 업데이트를 위해 단일 *IP* 주소를 발급합니다. *Panorama*가 기존 및 신규 관리 디바이스와 로그 수집기에 성공적으로 액세스할 수 있도록 인터넷에 연결된 외부 *IP* 주소를 입력하십시오. 내부 *Panorama IP* 주소가 구성된 경우 일부 디바이스를 관리하지 못할 수 있습니다. 예를 들어 AWS에 Panorama 설치(을)를 수행하고 내부 *IP* 주소를 입력하면 *Panorama*는 *AWS* 보안 그룹 외부의 디바이스 또는 로그 수집기를 관리할 수 없습니다.
   4. (선택 사항) Panorama에서 고가용성(HA) 쌍을 구성한 경우 두 번째 필드에 보조 Panorama의 IP 주소를 입력합니다.
   5. Panorama에서 생성한 인증 키를 입력합니다.
   6. 확인을 클릭합니다.



   7. 변경 사항을 커밋합니다.

STEP 5 | (선택 사항) 태그를 추가합니다. 태그를 사용하면 많은 목록에서 방화벽을 더 쉽게 찾을 수 있습니다. 디스플레이에서 방화벽 목록을 동적으로 필터링하고 구체화하는 데 도움이 됩니다. 예를 들어 ##이라는 태그를 추가하면 네트워크의 모든 지점 방화벽을 필터링할 수 있습니다.

1. 각 방화벽을 선택하고태그를 클릭합니다.
2. 추가를 클릭하고 최대 31자의 문자열을 입력하고(공백 없이) 확인을 클릭합니다.

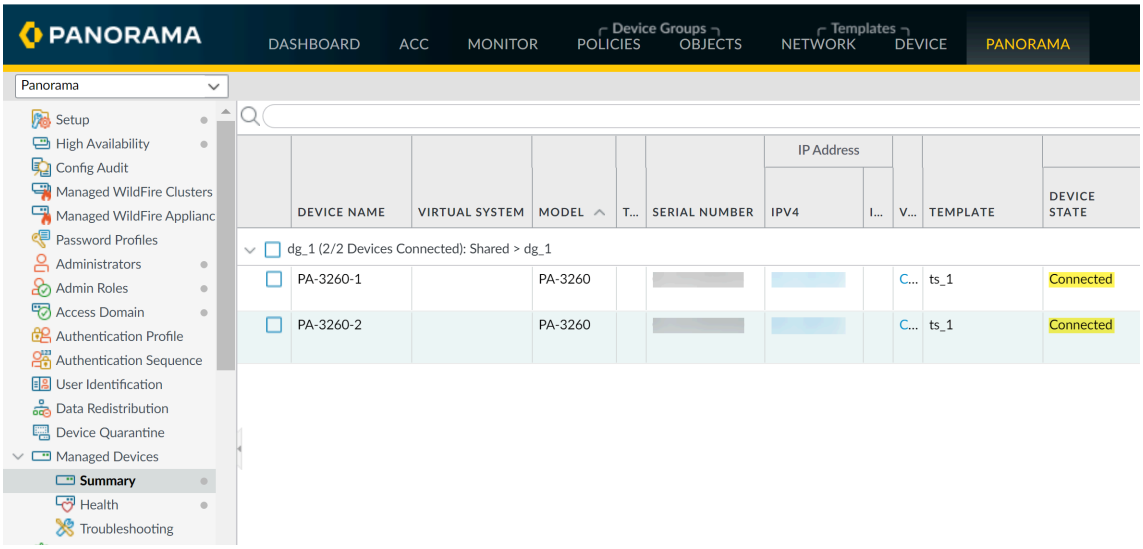
©2024 Palo Alto Networks, Inc.

STEP 6 | 배포에서 Panorama와 관리되는 디바이스 간의 인증을 위해 사용자 지정 인증서를 사용하는 경우 사용자 지정 클라이언트 디바이스 인증서를 배포합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정 및 새 클라이언트 디바이스 추가를 참조하십시오.

STEP 7 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

STEP 8 | 방화벽이 Panorama에 연결되어 있는지 확인합니다.

1. **Panorama** > 관리되는 디바이스 > 요약을 클릭합니다.
2. 새 디바이스의 디바이스 상태가 ###으로 표시되는지 확인합니다.



 ©2024 Palo Alto Networks, Inc.

관리 방화벽에 대한 디바이스 인증서 설치

하나 이상의 Palo Alto Networks 클라우드 서비스를 사용하려면 관리형 방화벽에 디바이스 인증서를 설치합니다. 단일 관리 방화벽 또는 여러 관리 방화벽에 대한 디바이스 인증서를 한 번에 설치할 수 있습니다.

방화벽 디바이스 인증서를 로컬로 설치하려면 디바이스 인증서를 참조하십시오.

- 관리 방화벽에 대한 디바이스 인증서 설치
- 디바이스 인증서가 없는 모든 관리형 방화벽에 대한 디바이스 인증서 설치

관리 방화벽에 대한 디바이스 인증서 설치

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• NGFW (Managed by Panorama)	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스 ❑ 아웃바운드 인터넷 액세스 ❑ 다음 사용자 역할 중 하나를 가진 고객 지원 포털(CSP) 계정: 수퍼유저, 표준 사용자, 제한된 사용자, 위협 연구원, AutoFocus 평가판 역할, 그룹 수퍼유저, 그룹 표준 사용자, 그룹 제한된 사용자, 그룹 위협 연구원, 승인된 지원 센터(ASC) 사용자 및 ASC 전체 서비스 사용자 ❑ Panorama 수퍼유저 역할

Panorama 관리 서버에서 관리형 방화벽에 대한 디바이스 인증서를 선택하고 설치하여 하나 이상의 클라우드 서비스를 사용합니다. 디바이스 인증서는 한 번만 설치하면 됩니다. 디바이스 인증서의 수명은 90일입니다. 방화벽은 인증서가 만료되기 15일 전에 디바이스 인증서를 다시 설치합니다. 방화벽이 로그 수집기가 자체적으로 디바이스 인증서를 다시 설치할 수 없는 경우 수동으로 만료된 디바이스 인증서를 복원해야 할 수도 있습니다.

방화벽에 디바이스 인증서를 성공적으로 설치하려면 방화벽에 아웃바운드 인터넷 액세스가 있어야 하며 CSP에 연결하려면 네트워크에서 다음 정규화된 도메인 이름(FQDN) 및 포트를 허용해야 합니다. 또한 관리형 방화벽이 디바이스 인증서를 설치하는 데 사용되는 One Time Password(OTP)를 생성하려면 Panorama와 동일한 CSP 계정에 있어야 합니다.

FQDN	포트
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com	TCP 80

©2024 Palo Alto Networks, Inc.

FQDN	포트
• http://ocsp.godaddy.com	
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 및 TCP 443

다음 *Palo Alto Networks* 차세대 방화벽 모델은 초기 등록 프로세스 중 *Palo Alto Networks CSP*에 처음 연결할 때 디바이스 인증서를 설치합니다. 이러한 방화벽 모델의 경우 디바이스 인증서를 수동으로 설치할 필요가 없습니다.

- *PA-400 Series* 방화벽
- *PA-1400 Series* 방화벽
- *PA-3400* 시리즈 방화벽
- *PA-5400* 시리즈 방화벽
- *PA-5450* 방화벽

STEP 1 | 수퍼유저로 Panorama 웹 인터페이스에 로그인합니다.

OTP 요청 토큰을 생성하고 관리형 방화벽에 디바이스 인증서를 설치하는 데 사용되는 OTP를 적용하려면 수퍼유저 액세스 권한이 있는 Panorama 관리자가 필요합니다.

STEP 2 | (모범 사례) Panorama에 대한 Network Time Protocol(NTP) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. **Panorama** > 설정 > 서비스를 선택합니다.
2. **NTP**를 선택하고 기본 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
3. (선택 사항) 보조 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
4. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) - NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID 입력(1-65534)

 ©2024 Palo Alto Networks, Inc.

- 알고리즘 - NTP 인증(**MDS** 또는 **SHA1**)에 사용할 알고리즘을 선택합니다.

5. 확인을 클릭하여 구성 변경 사항을 저장합니다.
6. 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 3 | 방화벽에 대한 Network Time Protocol(NTP) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. 디바이스 > 설정 > 서비스를 선택한 다음 템플릿을 선택합니다.
2. 플랫폼에 따라 다음 중 하나를 선택합니다.
   - 다중 가상 시스템 플랫폼의 경우 전역을 선택한 다음 서비스 섹션을 편집합니다.
   - 단일 가상 시스템 플랫폼의 경우 서비스 섹션을 편집합니다.
3. **NTP**를 선택하고 기본 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
4. (선택 사항) 보조 **NTP** 서버의 호스트 이름 또는 IP 주소를 입력합니다.
5. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) - NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID 입력(1-65534)
     - 알고리즘 - NTP 인증(**MDS** 또는 **SHA1**)에 사용할 알고리즘을 선택합니다.
6. 확인을 클릭하여 구성 변경 사항을 저장합니다.
7. 커밋 및 커밋 및 푸시를 선택한 다음 구성 변경 사항을 관리형 방화벽에 푸시합니다.

STEP 4 | Panorama에서 OTP 요청 토큰을 생성합니다.

Panorama에서 생성된 OTP 요청 토큰은 관리형 방화벽에 디바이스 인증서를 설치하는 데 필요한 OTP를 생성하는 데 사용됩니다.

1. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
2. 디바이스 인증서를 설치하지 않은 하나 이상의 관리형 방화벽을 선택합니다.
3. **CSP**에서 **OTP** 요청 > 사용자 지정 선택 디바이스를 선택합니다.
4. OTP 요청 토큰 필드에서 전체 출력을 복사합니다.

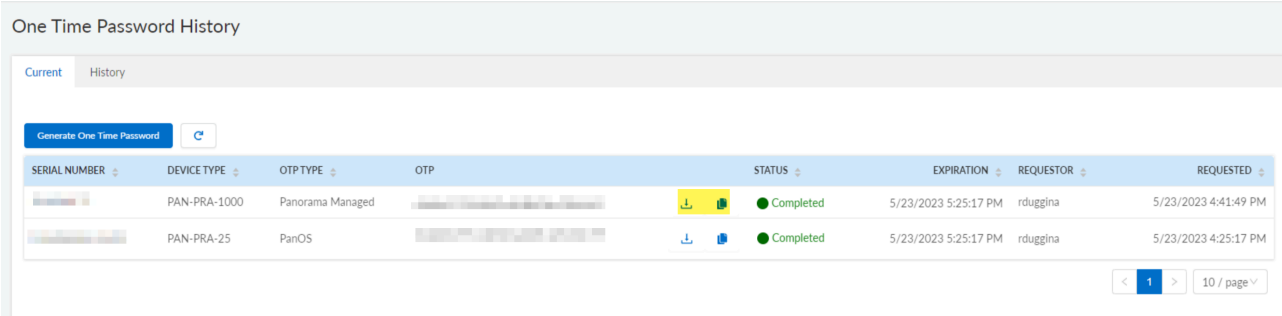
 ©2024 Palo Alto Networks, Inc.

STEP 5 | 관리형 방화벽에 대한 OTP(일회용 암호)를 생성합니다.

OTP 수명은 *60*분이며 *60*분 수명 내에 사용하지 않으면 만료됩니다.

방화벽은 *CSP*에서 *OTP* 검색을 한 번만 시도할 수 있습니다. 어떤 이유로든 방화벽이 *OTP*를 가져오는 데 실패하면 *OTP*가 만료되어 새 *OTP*를 생성해야 합니다.

1. OTP 생성 권한이 있는 사용자 역할로 고객 지원 포털에 로그인합니다.
2. 제품 > 디바이스 인증서를 선택하고 **OTP** 생성을 선택합니다.
3. 디바이스 유형에서 **Panorama** 관리형 방화벽용 **OTP** 생성을 선택하고 다음을 클릭합니다.
4. 이전 단계에서 복사한 OTP 요청을 붙여넣고 **OTP**를 생성합니다.
5. 완료를 클릭하고 OTP가 성공적으로 생성될 때까지 몇 분 정도 기다립니다.
6. **OTP** 기록을 확인합니다.
7. 현재 One-Time Password(OTP) 기록에서 OTP를 복사하거나 다운로드합니다.
8. 클립보드에 복사하거나 OTP를 다운로드합니다.



STEP 6 | 관리형 방화벽에 디바이스 인증서를 설치합니다.

관리형 방화벽이 디바이스 인증서를 성공적으로 설치하려면 아웃바운드 인터넷 연결이 있어야 합니다. Panorama에서 OTP를 업로드하면 관리형 방화벽이 Palo Alto Networks CSP에 연결하여 디바이스 인증서를 설치합니다.

1. 수퍼유저 사용자로 Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택한 다음 **OTP** 업로드를 선택합니다.
3. 생성한 OTP를 붙여넣고 업로드합니다.

이전 단계에서 *OTP*를 다운로드한 경우에도 *Palo Alto Networks CSP*에서 생성한 *OTP*를 복사하여 붙여넣어야 합니다. *OTP*가 포함된 파일 업로드는 지원되지 않습니다.

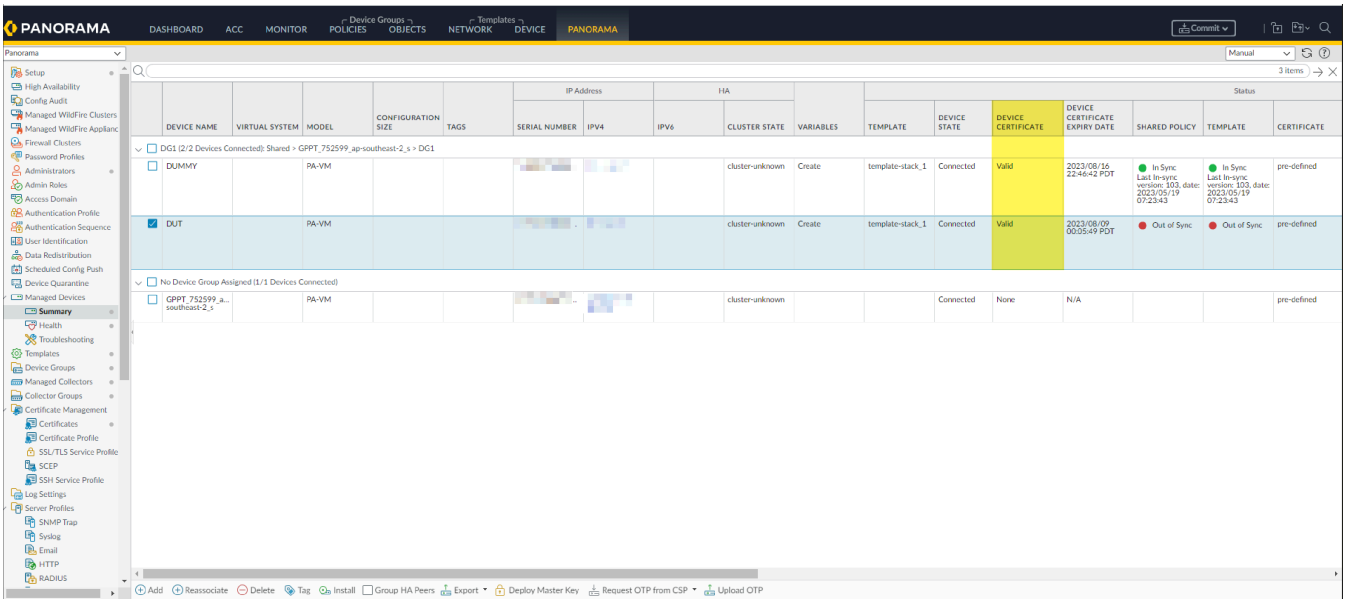
STEP 7 | (WildFire 및 Advanced WildFire) 방화벽 CLI에 로그인하고 방화벽 설정을 새로 고쳐 업데이트된 디바이스 인증서로 Advanced WildFire 클라우드에 대한 연결을 설정합니다.

Advanced WildFire 클라우드 서비스와 활성화된 WildFire 또는 Advanced WildFire 구독을 사용하는 각 관리 방화벽에 대해 이 단계를 반복합니다.

```
admin>request wildfire registration channel public
```


©2024 Palo Alto Networks, Inc.

STEP 8 | 디바이스 인증서 열이 ##로 표시되고 디바이스 인증서 만료 날짜가 만료 날짜를 표시하는지 확인합니다.



디바이스 인증서가 없는 모든 관리형 방화벽에 대한 디바이스 인증서 설치

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• NGFW (Managed by Panorama)	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스 ❑ 아웃바운드 인터넷 액세스 ❑ 다음 사용자 역할 중 하나를 가진 고객 지원 포털(CSP) 계정: 수퍼유저, 표준 사용자, 제한된 사용자, 위협 연구원, AutoFocus 평가판 역할, 그룹 수퍼유저, 그룹 표준 사용자, 그룹 제한된 사용자, 그룹 위협 연구원, 승인된 지원 센터(ASC) 사용자 및 ASC 전체 서비스 사용자 ❑ Panorama 수퍼유저 역할

Panorama 관리 서버에서 디바이스 인증서가 아직 설치되지 않은 관리형 방화벽에 대한 디바이스 인증서를 설치합니다. Palo Alto Networks CSP로 관리형 방화벽을 성공적으로 인증하고 하나 이상의 클라우드 서비스를 활용하려면 디바이스 인증서가 필요합니다. 디바이스 인증서의 수명은 90일입니다. 방화벽은 인증서가 만료되기 15일 전에 디바이스 인증서를 다시 설치합니다. 방화벽이 로그 수집기가 자체적으로 디바이스 인증서를 다시 설치할 수 없는 경우 수동으로 만료된 디바이스 인증서를 복원해야 할 수도 있습니다.

©2024 Palo Alto Networks, Inc.

관리형 방화벽에 대한 디바이스 인증서를 성공적으로 설치하려면 관리형 방화벽에 아웃바운드 인터넷 액세스가 있어야 하며 다음 FQDN(정규화된 도메인 이름) 및 포트가 네트워크에서 허용되어야 합니다. 또한 관리형 방화벽이 디바이스 인증서를 설치하는 데 사용되는 One Time Password(OTP)를 생성하려면 Panorama와 동일한 CSP 계정에 있어야 합니다.

FQDN	포트
• http://ocsp.paloaltonetworks.com • http://crl.paloaltonetworks.com • http://ocsp.godaddy.com	TCP 80
• https://api.paloaltonetworks.com • http://apitrusted.paloaltonetworks.com • https://certificatetrusted.paloaltonetworks.com • https://certificate.paloaltonetworks.com	TCP 443
• *.gpcloudservice.com	TCP 444 및 TCP 443

다음 *Palo Alto Networks* 차세대 방화벽 모델은 초기 등록 프로세스 중 *Palo Alto Networks CSP*에 처음 연결할 때 디바이스 인증서를 설치합니다. 이러한 방화벽 모델의 경우 디바이스 인증서를 수동으로 설치할 필요가 없습니다.

- *PA-400 Series* 방화벽
- *PA-1400 Series* 방화벽
- *PA-3400* 시리즈 방화벽
- *PA-5400* 시리즈 방화벽
- *PA-5450* 방화벽

STEP 1 | 수퍼유저로 Panorama 웹 인터페이스에 로그인합니다.

OTP 요청 토큰을 생성하고 관리형 방화벽에 디바이스 인증서를 설치하는 데 사용되는 OTP를 적용하려면 수퍼유저 액세스 권한이 있는 Panorama 관리자가 필요합니다.

STEP 2 | (모범 사례) Panorama에 대한 Network Time Protocol(NTP) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. **Panorama** > 설정 > 서비스를 선택합니다.

 ©2024 Palo Alto Networks, Inc.

2. **NTP**를 선택한 다음 호스트 이름 **pool.ntp.org**를 기본 **NTP** 서버로 입력하거나 기본 NTP 서버의 IP 주소를 입력합니다.
3. (선택 사항) 보조 **NTP** 서버 주소를 입력합니다.
4. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) - NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID 입력(1-65534)
     - 알고리즘 - NTP 인증(**MDS** 또는 **SHA1**)에 사용할 알고리즘을 선택합니다.
5. 확인을 클릭하여 구성 변경 사항을 저장합니다.
6. 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 3 | NTP(네트워크 시간 프로토콜) 서버를 구성합니다.

NTP 서버는 디바이스 인증 만료 날짜를 확인하고 디바이스 인증서가 조기에 만료되거나 무효화되지 않도록 해야 합니다.

1. 디바이스 > 설정 > 서비스를 선택한 다음 템플릿을 선택합니다.
2. 플랫폼에 따라 다음 중 하나를 선택합니다.
   - 다중 가상 시스템 플랫폼의 경우 전역을 선택한 다음 서비스 섹션을 편집합니다.
   - 단일 가상 시스템 플랫폼의 경우 서비스 섹션을 편집합니다.
3. **NTP**를 선택한 다음 호스트 이름 **pool.ntp.org**를 기본 **NTP** 서버로 입력하거나 기본 NTP 서버의 IP 주소를 입력합니다.
4. (선택 사항) 보조 **NTP** 서버 주소를 입력합니다.
5. (선택 사항) 인증 유형에 대해 NTP 서버에서 시간 업데이트를 인증하려면 각 서버에 대해 다음 중 하나를 선택합니다.
   - 없음(기본값) - NTP 인증을 비활성화합니다.
   - 대칭 키 - 방화벽은 대칭 키 교환(공유 암호)을 사용하여 시간 업데이트를 인증합니다.
     - 키 **ID** - 키 ID 입력(1-65534)
     - 알고리즘 - NTP 인증(**MDS** 또는 **SHA1**)에 사용할 알고리즘을 선택합니다.
6. 확인을 클릭하여 구성 변경 사항을 저장합니다.
7. 커밋 및 커밋 및 푸시를 선택한 다음 구성 변경 사항을 관리형 방화벽에 푸시합니다.

STEP 4 | Panorama에서 OTP 요청 토큰을 생성합니다.

Panorama에서 생성된 OTP 요청 토큰은 관리형 방화벽에 디바이스 인증서를 설치하는 데 필요한 OTP를 생성하는 데 사용됩니다.

1. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
2. **CSP**에서 **OTP** 요청 > 인증서가 없는 모든 디바이스 선택을 선택합니다.
3. OTP 요청 토큰 필드에서 전체 출력을 복사합니다.

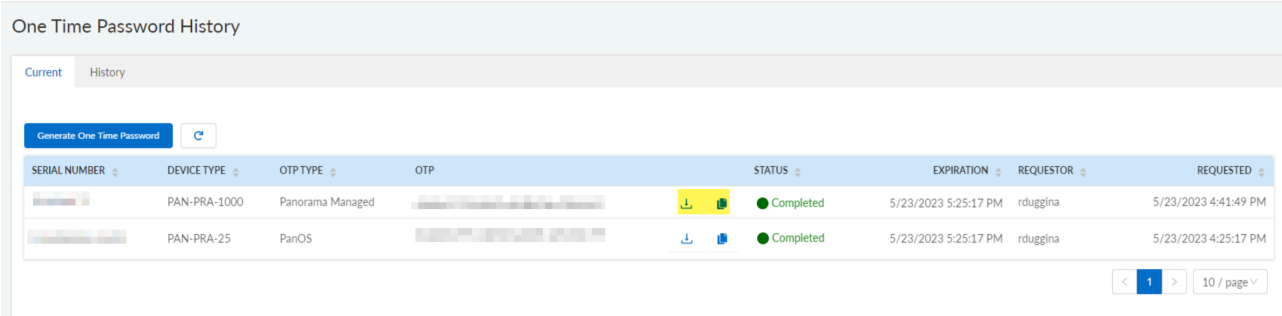
 ©2024 Palo Alto Networks, Inc.

STEP 5 | 관리형 방화벽에 대한 OTP(일회용 암호)를 생성합니다.

OTP 수명은 *60*분이며 *60*분 수명 내에 사용하지 않으면 만료됩니다.

방화벽은 *CSP*에서 *OTP* 검색을 한 번만 시도할 수 있습니다. 어떤 이유로든 방화벽이 *OTP*를 가져오는 데 실패하면 *OTP*가 만료되어 새 *OTP*를 생성해야 합니다.

1. OTP 생성 권한이 있는 사용자 역할로 고객 지원 포털에 로그인합니다.
2. 제품 > 디바이스 인증서를 선택하고 **OTP** 생성을 선택합니다.
3. 디바이스 유형에서 **Panorama** 관리형 방화벽용 **OTP** 생성을 선택하고 다음을 클릭합니다.
4. 이전 단계에서 복사한 OTP 요청을 붙여넣고 **OTP**를 생성합니다.
5. 완료를 클릭하고 OTP가 성공적으로 생성될 때까지 몇 분 정도 기다립니다.
6. **OTP** 기록을 확인합니다.
7. 현재 One-Time Password(OTP) 기록에서 OTP를 복사하거나 다운로드합니다.
8. 클립보드에 복사하거나 OTP를 다운로드합니다.



STEP 6 | 관리형 방화벽에 디바이스 인증서를 설치합니다.

관리형 방화벽이 디바이스 인증서를 성공적으로 설치하려면 아웃바운드 인터넷 연결이 있어야 합니다. Panorama에서 OTP를 업로드하면 관리형 방화벽이 Palo Alto Networks CSP에 연결하여 디바이스 인증서를 설치합니다.

1. 수퍼유저 사용자로 Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택한 다음 **OTP** 업로드를 선택합니다.
3. 생성한 OTP를 붙여넣고 업로드합니다.

이전 단계에서 *OTP*를 다운로드한 경우에도 *Palo Alto Networks CSP*에서 생성한 *OTP*를 복사하여 붙여넣어야 합니다. *OTP*가 포함된 파일 업로드는 지원되지 않습니다.

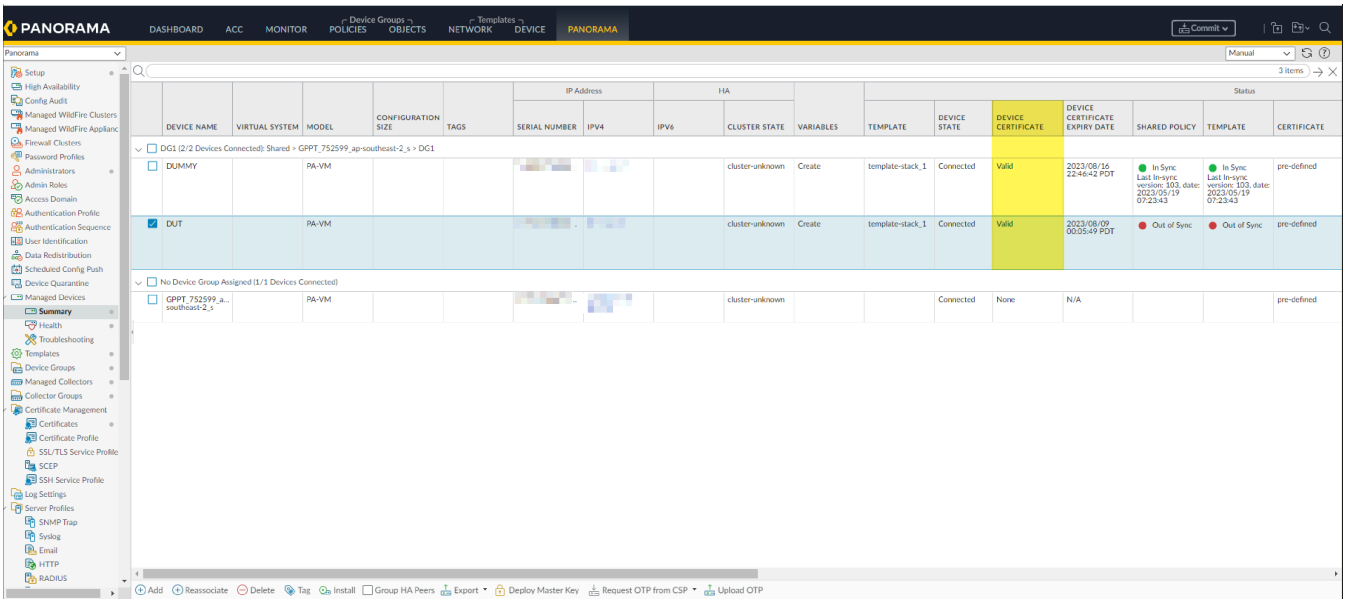
STEP 7 | (WildFire 및 Advanced WildFire) 방화벽 CLI에 로그인하고 방화벽 설정을 새로 고쳐 업데이트된 디바이스 인증서로 Advanced WildFire 클라우드에 대한 연결을 설정합니다.

Advanced WildFire 클라우드 서비스와 활성화된 WildFire 또는 Advanced WildFire 구독을 사용하는 각 관리 방화벽에 대해 이 단계를 반복합니다.

```
admin>request wildfire registration channel public
```


©2024 Palo Alto Networks, Inc.

STEP 8 | 디바이스 인증서 열이 ##로 표시되고 디바이스 인증서 만료 날짜가 만료 날짜를 표시하는지 확인합니다.



 ©2024 Palo Alto Networks, Inc.

Panorama 관리와 클라우드 관리 간의 변경 사항

아래 절차에서는 관리형 방화벽 관리 플랫폼을 Panorama™ 관리 서버에서 클라우드 관리로 변경하는 방법과 클라우드 관리에서 Panorama 관리로 변경하는 방법을 설명합니다.

Panorama 관리에서 클라우드 관리로 변경

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 클라우드 관리로 이동할 관리형 방화벽에 대한 로그 전달 환경 설정을 제거합니다.

1. **Panorama** > 수집기 그룹을 선택하고 관리형 방화벽이 연결된 수집기 그룹을 클릭합니다.
2. 디바이스 로그 전달을 선택합니다.
3. 클라우드 관리로 이동하려는 관리형 방화벽을 선택(체크)하고 삭제합니다.

   둘 이상의 관리형 방화벽을 클라우드 관리로 이동할 때 여러 방화벽을 선택(체크 수 있습니다.
4. 확인을 클릭합니다.
5. 커밋 및 **Panorama**에 커밋.

STEP 3 | 방화벽에서 관리 설정을 지정합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
3. 관리 대상으로 클라우드 서비스를 선택합니다.
4. 확인을 클릭합니다.
5. 커밋합니다.

STEP 4 | 방화벽을 클라우드 관리에 계속 온보딩합니다.

클라우드 관리에서 Panorama 관리로 변경

이는 방화벽의 클라우드 관리가 지원되지 않는 PAN-OS 10.2.2 또는 이전 릴리스로 관리 방화벽을 다운그레이드하는 경우에도 필요합니다.

STEP 1 | 방화벽에서 관리 설정을 지정합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
3. 관리자에서 **Panorama**를 선택합니다.

   원래 추가한 Panorama IP 및 디바이스 등록 인증 키는 여전히 구성되어 있어야 합니다. 그렇지 않은 경우 관리형 방화벽을 Panorama에 다시 추가하는 방법에 대한 자세한 내용은 관리되는 디바이스로 방화벽 추가에서 확인할 수 있습니다.
4. 확인을 클릭합니다.
5. 커밋합니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | 관리형 방화벽에서 관리 플레인을 다시 시작합니다.

1. 방화벽 CLI에 로그인합니다.
2. 관리 플레인을 다시 시작합니다.

```
admin>  debug software restart process management-server
```

STEP 3 | 관리형 방화벽이 Panorama에 성공적으로 연결되었는지 확인합니다.

1. Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 관리형 디바이스 > 요약을 선택하고 관리형 방화벽 상태가 ###인지 확인합니다.

©2024 Palo Alto Networks, Inc.

제로 터치 프로비저닝 설정

ZTP(Zero Touch Provisioning)를 설정하여 네트워크 관리자가 방화벽을 수동으로 프로비저닝할 필요 없이 새로운 관리형 방화벽 온보딩을 자동화하여 초기 방화벽 배포를 간소화하고 효율화합니다.

ZTP 온보딩에는 ZTP 방화벽이 필요하며 ZTP 방화벽의 전원을 켜기 전에 Eth1/1 인터페이스를 아웃바운드 인터넷 연결과 케이블로 연결해야 합니다. 이는 ZTP 방화벽을 Panorama 관리에 성공적으로 온보딩하고, ZTP 방화벽을 CSP에 등록하며, Panorama에서 정책 및 네트워크 구성을 푸시하는 데 필요합니다.

수퍼유저 권한이 있는 Panorama 관리자만 ZTP 설정에 필요한 ZTP 설정에 액세스할 수 있습니다.

ZTP 서비스를 성공적으로 활용하려면 *PAN-OS 10.0.0* 이상의 버전으로 업그레이드하기 전에 공장 기본 *PAN-OS* 버전으로 *ZTP* 방화벽을 온보드하십시오.

ZTP 플러그인은 *PAN-OS 9.1.4* 이상 릴리스에서 지원됩니다.

- ZTP 개요
- ZTP 플러그인 설치
- ZTP 설치 관리자 계정 구성
- Panorama에 ZTP 방화벽 추가
- ZTP 작업에 CLI 사용
- ZTP 플러그인 제거

ZTP 개요

ZTP(Zero Touch Provisioning) 및 해당 구성 요소에 대해 자세히 알아보십시오.

- ZTP 소개
- ZTP 구성 요소

ZTP 소개

ZTP(Zero Touch Provisioning)는 Panorama™ 관리 서버에 대한 새 방화벽의 온보딩을 단순화하고 자동화하도록 설계되었습니다. ZTP는 네트워크 관리자가 관리 방화벽을 분기로 직접 배송하고 ZTP 방화벽이 Palo Alto Networks ZTP 서비스에 성공적으로 연결된 후 Panorama™ 관리 서버에 방화벽을 자동으로 추가할 수 있도록 하여 초기 방화벽 배포 프로세스를 간소화합니다. 이를 통해 기업은 IT 관리자가 새로운 관리 방화벽을 수동으로 프로비저닝할 필요가 없어 지사에 새 방화벽을 배포할 때 시간과 리소스를 절약할 수 있습니다. 성공적인 온보딩 후 Panorama는 ZTP 구성 및 방화벽을 구성하고 관리하는 수단을 제공합니다.

ZTP 클라우드 서비스는 인터넷 직접 연결을 지원하여 ZTP 방화벽을 Panorama 관리에 성공적으로 온보딩할 수 있습니다. ZTP 클라우드 서비스는 명시적 웹 프록시를 지원하지 않으며, 명시적 웹 프록시가 ZTP 방화벽 및 Panorama의 인터넷 게이트웨이로 구성되어 있는 경우 ZTP 방화벽을 Panorama 관리로 온보딩할 수 없습니다.

예약된 유지 관리 기간, 중단 및 해결 방법에 대한 알림을 받을 ZTP 서비스 상태 이벤트를 검토하고 구독합니다.

©2024 Palo Alto Networks, Inc.

ZTP는 다음 ZTP 방화벽에서 지원됩니다.

- PA-400 시리즈 방화벽
- PA-820-ZTP 및 PA-850-ZTP
- PA-1400 시리즈 방화벽
- PA-3220-ZTP, PA-3250-ZTP 및 PA-3260-ZTP
- PA-3400 시리즈 방화벽
- PA-5400 시리즈 방화벽
- PA-5450

Panorama에서 ZTP 설정을 시작하기 전에 방화벽 하드웨어 빠른 시작 및 참조 가이드를 검토하여 ZTP를 성공적으로 활용하기 위해 방화벽을 올바르게 설치하는 방법을 이해하십시오.

ZTP 구성 요소

다음 요소가 함께 작동하여 ZTP 서비스를 사용하여 Panorama 관리 서버에 자동으로 추가하여 새로 배포된 ZTP 방화벽을 신속하게 온보딩할 수 있습니다.

- **ZTP** 플러그인 - ZTP 플러그인을 사용하면 Panorama가 ZTP 서비스에 연결하고 온보딩 간소화를 위해 ZTP 방화벽을 요청할 수 있습니다.
- 고객 지원 포털**(CSP)** - Palo Alto Networks 고객 지원 포털은 새로 추가된 ZTP 방화벽을 자동으로 등록하기 위해 CSP에 연결할 Panorama를 등록하는 데 사용됩니다.
- 일회용 비밀번호**(OTP)** - CSP 및 ZTP 서비스와 통신하기 위해 Panorama에서 인증서를 검색하고 설치하는 데 사용되는 Palo Alto Networks에서 제공하는 일회용 비밀번호입니다.
- 설치 관리자 - ZTP 방화벽 온보딩을 위해 `installeradmin` 관리자 역할을 사용하여 생성된 관리자 사용자입니다. 이 관리자는 Panorama 웹 인터페이스에 대한 액세스가 제한되어 있으며 CSP 및 Panorama에 방화벽을 등록하기 위한 ZTP 방화벽 일련번호 및 클레임 키 입력에 대한 액세스만 허용합니다. 설치 관리자 관리자는 Panorama에서 생성하거나 RADIUS, SAML 또는 TACACS+와 같은 원격 인증을 사용하여 생성할 수 있습니다.
- 클레임 키 - ZTP 방화벽을 CSP에 등록하는 데 사용되는 ZTP 방화벽에 물리적으로 연결된 8자리 숫자 키입니다.
- **To-SW-Version** - ZTP 방화벽의 PAN-OS 소프트웨어 버전을 지정합니다**(Panorama > Managed Devices > Summary)**. 대상 PAN-OS 버전을 선택한 다음 방화벽이 표시된 버전보다 이전 버전을 실행 중인 경우 방화벽은 대상 버전이 성공적으로 설치될 때까지 업그레이드 루프를 시작합니다.

> *Panorama*는 *Panorama*에 설치된 것과 같거나 그 이하의 *PAN-OS* 버전을 실행하는 방화벽만 관리할 수 있습니다.

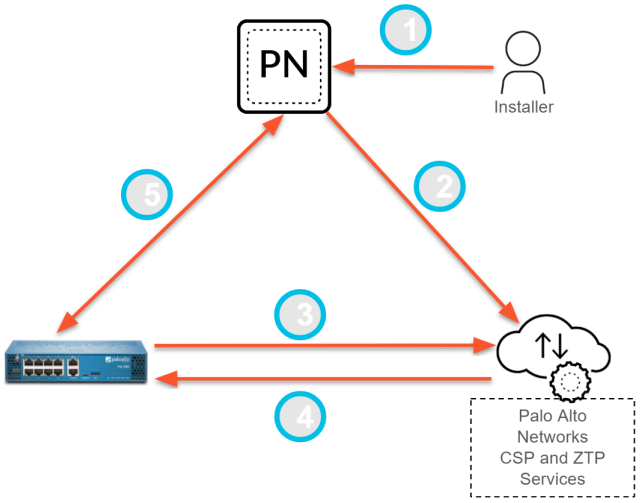
Panorama에 ZTP 플러그인을 성공적으로 설치하고 ZTP 서비스에 Panorama를 등록한 후 ZTP 탑승 프로세스는 다음과 같이 계속됩니다.

1. 설치자 또는 IT 관리자는 방화벽 일련번호와 클레임 키를 사용하여 ZTP 방화벽을 Panorama에 추가하여 등록합니다.

 ©2024 Palo Alto Networks, Inc.

2. Panorama는 방화벽을 CSP에 등록합니다. 방화벽이 성공적으로 등록되면 방화벽은 ZTP 서비스의 Panorama와 동일한 ZTP 테넌트와 연결됩니다.

   ZTP 서비스에 성공적으로 등록된 ZTP 방화벽은 Panorama에서 관리 방화벽(**Panorama** > **Managed Devices**)으로 자동 추가됩니다.
3. 방화벽이 인터넷에 연결되면 ZTP 방화벽은 ZTP 서비스에 연결하기 위해 CSP에 디바이스 인증서를 요청합니다.
4. ZTP 서비스는 Panorama IP 또는 FQDN을 ZTP 방화벽으로 푸시합니다.
5. ZTP 방화벽은 Panorama에 연결되고 디바이스 그룹 및 템플릿 구성은 Panorama에서 ZTP 방화벽으로 푸시됩니다.



ZTP 플러그인 설치

Panorama™ 관리 서버에 ZTP 플러그인을 설치하여 Panorama를 ZTP 서비스에 등록하여 온보딩 간소화를 위한 ZTP 방화벽을 신청하세요.

Panorama가 고가용성(HA) 구성인 경우 ZTP 플러그인을 설치하고 두 Panorama HA 피어를 ZTP 서비스에 등록합니다.

- Panorama에 ZTP 플러그인 설치
- ZTP 서비스에 Panorama 등록

Panorama에 ZTP 플러그인 설치

Panorama 관리 서버에 ZTP 플러그인을 설치하여 ZTP 방화벽의 온보딩 및 관리를 간소화합니다.

STEP 1 | Panorama 디바이스 인증서 설치.

STEP 2 | Panorama 웹 인터페이스에 수퍼유저 또는 Panorama 관리자로 로그인하여 Panorama 플러그인(**Panorama** > 플러그인)에 액세스합니다.

STEP 3 | **Panorama** > 플러그인을 선택한 다음 **`ztp`** 플러그인을 검색합니다.

STEP 4 | 최신 버전의 ZTP 플러그인을 다운로드하여 설치합니다.

©2024 Palo Alto Networks, Inc.

ZTP 서비스에 Panorama 등록

신규 및 기존 배포를 위해 Panorama™ 관리 서버를 ZTP 서비스에 등록합니다.

- 새 배포를 위해 ZTP 서비스에 Panorama 등록
- 기존 배포용 ZTP 서비스에 Panorama 등록

새 배포를 위해 ZTP 서비스에 Panorama 등록

Panorama™ 관리 서버에 ZTP 플러그인을 설치한 후에는 ZTP 서비스가 방화벽을 Panorama와 연결할 수 있도록 Panorama를 ZTP 서비스에 등록해야 합니다. ZTP 새 배포를 위한 등록 프로세스의 일부로 ZTP 방화벽을 ZTP 서비스에 연결하는 데 필요한 디바이스 그룹 및 템플릿 구성을 자동으로 생성합니다. 디바이스 그룹 및 템플릿이 자동으로 생성된 후에는 먼저 Panorama에 연결된 후 ZTP 서비스에 연결할 수 있도록 디바이스 그룹 및 템플릿에 ZTP 방화벽을 추가해야 합니다.

STEP 1 | Panorama 디바이스 인증서 설치.

STEP 2 | Palo Alto Networks 고객 지원 포털(CSP)에 로그인합니다.

STEP 3 | Panorama를 Palo Alto Networks CSP의 ZTP 서비스와 연결합니다.

ZTP 서비스는 고가용성(HA) 구성에 있는 경우에만 최대 2개의 Panorama 연결을 지원합니다. Panorama가 HA 구성에 없는 경우 단일 Panorama만 연결할 수 있습니다.

1. 자산 > **ZTP** 서비스를 선택한 다음 **Panorama**를 연결합니다.
2. ZTP 방화벽을 관리하는 Panorama의 일련번호를 선택합니다.
3. (HA만 해당) Panorama HA 피어의 일련번호를 선택합니다.
4. 확인을 클릭합니다.

STEP 4 | Panorama에서 **Panorama** > **Zero Touch Provisioning** > 설정을 선택하고 일반 ZTP 설정을 편집합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | ZTP 서비스에 Panorama를 등록하세요.

1. **ZTP** 서비스를 활성화합니다.
2. **Panorama FQDN** 또는 **IP** 주소를 입력합니다.

   이것은 ZTP 플러그인이 설치되고 CSP가 ZTP 방화벽으로 푸시하는 Panorama의 FQDN 또는 공용 IP 주소입니다.

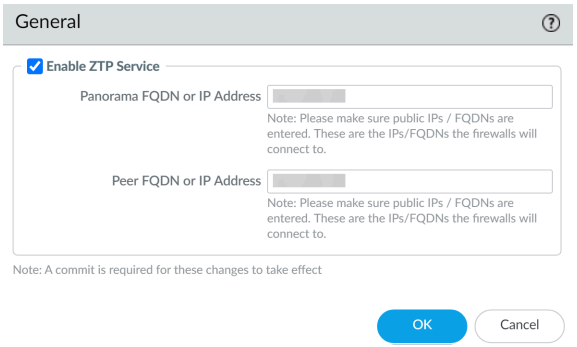
   (*PAN-OS 10.1.4* 및 이전 릴리스를 실행하는 관리형 방화벽) 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되는 것을 방지하려면 *Panorama IP* 주소를 입력합니다.

   *Panorama FQDN*을 사용해야 하는 경우 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되지 않도록 정적 대상 경로를 구성합니다.
3. (HA만 해당) 피어 **FQDN** 또는 **IP** 주소를 입력합니다.

   이것은 ZTP 플러그인이 설치된 Panorama 피어의 FQDN 또는 공용 IP 주소이며 페일오버의 경우 CSP가 ZTP 방화벽으로 푸시합니다.

   (*PAN-OS 10.1.4* 및 이전 릴리스를 실행하는 관리형 방화벽) 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되는 것을 방지하려면 *Panorama IP* 주소를 입력합니다.

   *Panorama FQDN*을 사용해야 하는 경우 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되지 않도록 정적 대상 경로를 구성합니다.
4. 확인을 클릭하여 구성 변경 사항을 저장합니다.



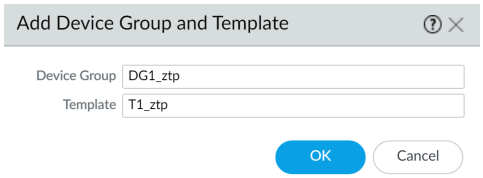
 ©2024 Palo Alto Networks, Inc.

STEP 6 | 기본 디바이스 그룹 및 템플릿을 생성하여 ZTP 방화벽을 Panorama에 연결하는 데 필요한 구성을 자동으로 생성합니다.

디바이스 그룹 및 템플릿을 추가하면 Panorama와 ZTP 방화벽을 연결하기 위한 기본 구성이 포함된 새 디바이스 그룹 및 템플릿이 자동으로 생성됩니다.

*Palo Alto Networks*는 *ZTP* 디바이스 그룹 및 템플릿에 목적을 명확하게 설명하는 설명 이름을 지정할 것을 권장합니다. 실수로 기본 *ZTP* 구성을 수정하면 나중에 디바이스 그룹 및 템플릿을 다시 사용하여 새 *ZTP* 방화벽을 온보딩하려는 경우 연결 문제가 발생합니다.

1. 디바이스 그룹 및 템플릿을 추가합니다.
2. 디바이스 그룹 이름을 입력합니다.
3. 템플릿 이름을 입력합니다.
4. 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 7 | 새 템플릿 스택(template stack)을 생성하고 이전 단계에서 생성된 템플릿을 추가합니다.

1. 템플릿을 선택하고 새 템플릿 스택(template stack)을 추가합니다.
2. 템플릿 스택(template stack)을 설명하는 이름을 입력합니다.
3. (PAN-OS 11.2 이상 릴리즈) 소프트웨어 디바이스가 **Panorama**에 등록되면 자동으로 콘텐츠 푸시를 선택(활성화)합니다.
4. 템플릿에 이전 단계에서 생성된 템플릿을 추가합니다.

STEP 8 | (PAN-OS 11.2 이상 릴리즈에 권장됨) 처음으로 Panorama에 성공적으로 연결할 때 ZTP 방화벽을 자동으로 설치하려면 최신 동적 콘텐츠 버전을 다운로드합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다.
2. ZTP 방화벽에 설치하려는 최신 동적 콘텐츠 버전을 다운로드합니다.

STEP 9 | 필요에 따라 ZTP 디바이스 그룹, 템플릿 및 템플릿 스택을 수정합니다.

ZTP 방화벽을 다른 디바이스 그룹 또는 템플릿 스택으로 이동하는 것은 지원되지 않습니다. ZTP 방화벽은 ZTP 디바이스 그룹 및 작성된 ZTP 템플릿을 포함하는 템플릿 스택에 보관해야 합니다. 이는 방화

©2024 Palo Alto Networks, Inc.

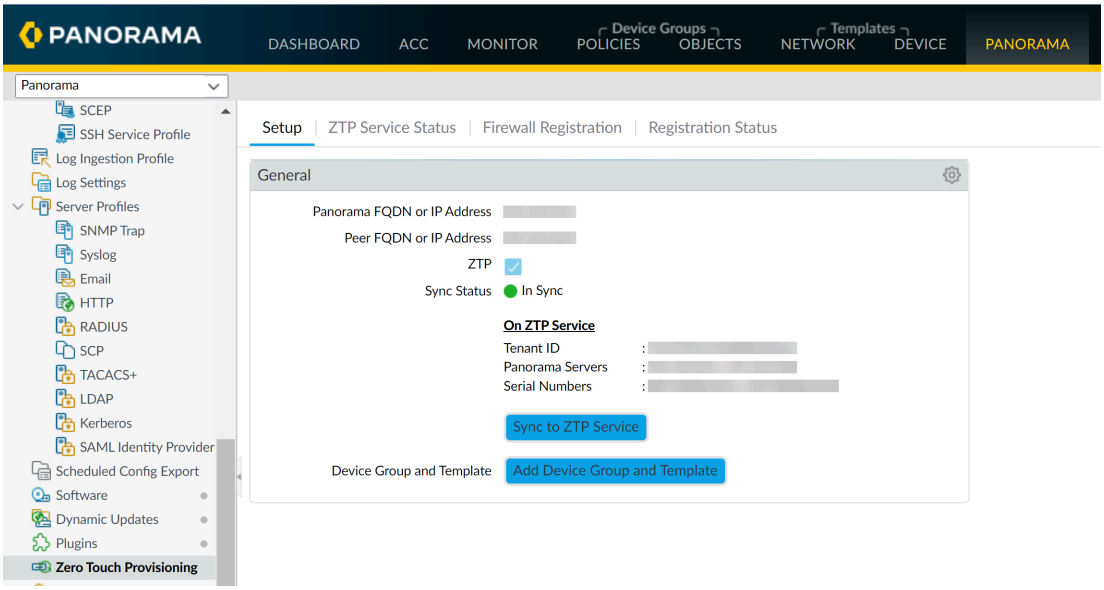
벽이 Panorama와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌리는 것을 방지하는 데 필요합니다.

템플릿 스택(template stack)에서 디바이스 그룹 계층과 템플릿 우선 순위를 고려할 때 ZTP 방화벽과 Panorama가 통신할 수 있도록 하는 필수 ZTP 구성이 포함된 템플릿과 디바이스 그룹에 우선 순위가 있어야 구성 충돌이 발생할 경우 구성이 무시되지 않습니다.

ZTP 방화벽을 온보딩하는 데 사용되는 *ZTP* 디바이스 그룹 및 템플릿을 수정하는 경우 이전 단계에서 디바이스 그룹 및 템플릿을 생성할 때 자동으로 채워진 *ZTP* 구성을 수정하지 않도록 주의합니다. 여기에는 *Panorama IP* 주소, 가상 라우터, `ethernet1/1` 인터페이스, `ethernet1/1` 인터페이스의 보안 영역, `loopback.900` 루프백 인터페이스, `rule1` 보안 정책 규칙, `ztp-nat` NAT 정책 규칙 및 서비스 경로와 같은 구성이 포함됩니다. 이러한 구성은 *ZTP* 방화벽을 *Panorama*에 연결하는 데 필요하며 수정하면 연결 문제가 발생할 수 있습니다.

STEP 10 | 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 11 | **ZTP** 서비스에 동기화하고 Panorama 동기화 상태가 ### #으로 표시되는지 확인합니다.



STEP 12 | Panorama에 ZTP 방화벽 추가.

기존 배포용 **ZTP** 서비스에 **Panorama** 등록

Panorama™ 관리 서버에 ZTP 플러그인을 설치한 후 ZTP 서비스가 방화벽을 Panorama와 연결할 수 있도록 Panorama를 ZTP 서비스에 등록해야 합니다. 등록 프로세스의 일부로 ZTP 방화벽이 Panorama에 처음 연결된 후 ZTP 방화벽을 ZTP 서비스와 연결하는 데 필요한 ZTP 구성이 포함된 기존 ZTP 디바이스 그룹 및 템플릿 스택에 ZTP 방화벽을 추가합니다.

STEP 1 | Panorama 디바이스 인증서 설치.

STEP 2 | Palo Alto Networks 고객 지원 포털(CSP)에 로그인합니다.

©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama를 Palo Alto Networks CSP의 ZTP 서비스와 연결합니다.

ZTP 서비스는 고가용성(HA) 구성에 있는 경우에만 최대 2개의 Panorama 연결을 지원합니다. Panorama가 HA 구성에 없는 경우 단일 Panorama만 연결할 수 있습니다.

1. 자산 > **ZTP** 서비스를 선택한 다음 연결 수정을 선택합니다.
2. ZTP 방화벽을 관리하는 Panorama의 일련번호를 선택합니다.
3. (HA만 해당) Panorama HA 피어의 일련번호를 선택합니다.
4. 확인을 클릭합니다.

STEP 4 | Panorama에서 **Panorama** > **Zero Touch Provisioning** > 설정을 선택하고 일반 ZTP 설정을 편집합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | ZTP 서비스에 Panorama를 등록하세요.

1. **ZTP** 서비스를 활성화합니다.
2. **Panorama FQDN** 또는 **IP** 주소를 입력합니다.

   이것은 ZTP 플러그인이 설치되고 CSP가 ZTP 방화벽으로 푸시하는 Panorama의 FQDN 또는 공용 IP 주소입니다.

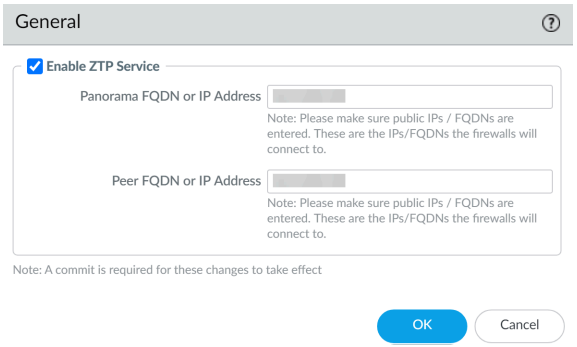
   (*PAN-OS 10.1.4* 및 이전 릴리스를 실행하는 관리형 방화벽) 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되는 것을 방지하려면 *Panorama IP* 주소를 입력합니다.

   *Panorama FQDN*을 사용해야 하는 경우 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되지 않도록 정적 대상 경로를 구성합니다.
3. (HA만 해당) 피어 **FQDN** 또는 **IP** 주소를 입력합니다.

   이것은 ZTP 플러그인이 설치된 Panorama 피어의 FQDN 또는 공용 IP 주소이며 페일오버의 경우 CSP가 ZTP 방화벽으로 푸시합니다.

   (*PAN-OS 10.1.4* 및 이전 릴리스를 실행하는 관리형 방화벽) 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되는 것을 방지하려면 *Panorama IP* 주소를 입력합니다.

   *Panorama FQDN*을 사용해야 하는 경우 재부팅 시 또는 성공적인 *PAN-OS* 업그레이드 후 관리형 방화벽이 *Panorama*에서 연결 해제되지 않도록 정적 대상 경로를 구성합니다.
4. 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 6 | 새 템플릿 스택(template stack)을 생성하고 이전 단계에서 생성된 템플릿을 추가합니다.

1. 템플릿을 선택하고 새 템플릿 스택(template stack)을 추가합니다.
2. 템플릿 스택(template stack)을 설명하는 이름을 입력합니다.
3. (PAN-OS 11.2 이상 릴리즈) 소프트웨어 디바이스가 **Panorama**에 등록되면 자동으로 콘텐츠 푸시를 선택(활성화)합니다.
4. 템플릿에 이전 단계에서 생성된 템플릿을 추가합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | (PAN-OS 11.2 이상 릴리즈에 권장됨) 처음으로 Panorama에 성공적으로 연결할 때 ZTP 방화벽을 자동으로 설치하려면 최신 동적 콘텐츠 버전을 다운로드합니다.

1. **Panorama** > 디바이스 배포 > 동적 업데이트 및 지금 확인을 선택합니다.
2. ZTP 방화벽에 설치하려는 최신 동적 콘텐츠 버전을 다운로드합니다.

STEP 8 | 필요에 따라 ZTP 디바이스 그룹, 템플릿 및 템플릿 스택을 수정합니다.

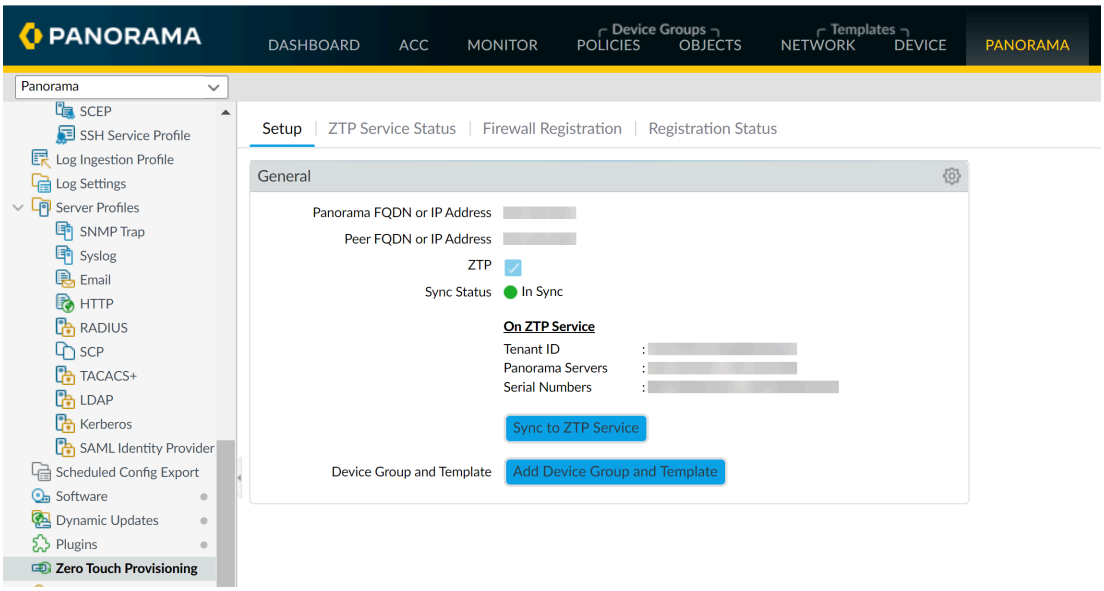
ZTP 방화벽을 다른 디바이스 그룹 또는 템플릿 스택으로 이동하는 것은 지원되지 않습니다. 생성된 ZTP 디바이스 그룹 및 템플릿에 ZTP 온보드 방화벽을 유지해야 합니다. 이는 방화벽이 Panorama와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌리는 것을 방지하는 데 필요합니다.

템플릿 스택(template stack)에서 디바이스 그룹 계층과 템플릿 우선 순위를 고려할 때 ZTP 방화벽과 Panorama가 통신할 수 있도록 하는 필수 ZTP 구성이 포함된 템플릿과 디바이스 그룹에 우선 순위가 있어야 구성 충돌이 발생할 경우 구성이 무시되지 않습니다.

ZTP 방화벽을 온보딩하는 데 사용되는 *ZTP* 디바이스 그룹 및 템플릿을 수정하는 경우 이전 단계에서 디바이스 그룹 및 템플릿을 생성할 때 자동으로 채워진 *ZTP* 구성을 수정하지 않도록 주의합니다. 여기에는 *Panorama IP* 주소, 가상 라우터, `ethernet1/1` 인터페이스, `ethernet1/1` 인터페이스의 보안 영역, `loopback.900` 루프백 인터페이스, `rule1` 보안 정책 규칙, `ztp-nat` *NAT* 정책 규칙 및 서비스 경로와 같은 구성이 포함됩니다. 이러한 구성은 *ZTP* 방화벽을 *Panorama*에 연결하는 데 필요하며 수정하면 연결 문제가 발생할 수 있습니다.

STEP 9 | 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 10 | **ZTP** 서비스에 동기화하고 Panorama 동기화 상태가 ### #으로 표시되는지 확인합니다.



STEP 11 | Panorama에 ZTP 방화벽 추가.

©2024 Palo Alto Networks, Inc.

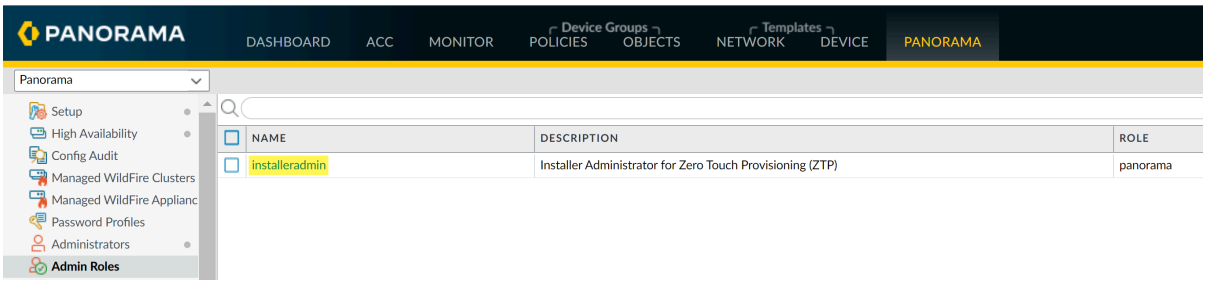
ZTP 설치 관리자 계정 구성

ZTP 설치 관리자 관리자 사용자는 IT 직원이 아니거나 설치 계약자가 새 ZTP 방화벽을 온보딩할 수 있도록 만든 관리자 계정입니다. 설치 관리자 관리자는 자동으로 생성된 `installeradmin` 관리자 역할을 사용하여 Panorama 웹 인터페이스에 대한 가시성을 제한하고 설치 관리자가 Panorama에 ZTP 방화벽 클레임 키 및 일련번호를 입력하는 기능만 허용합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

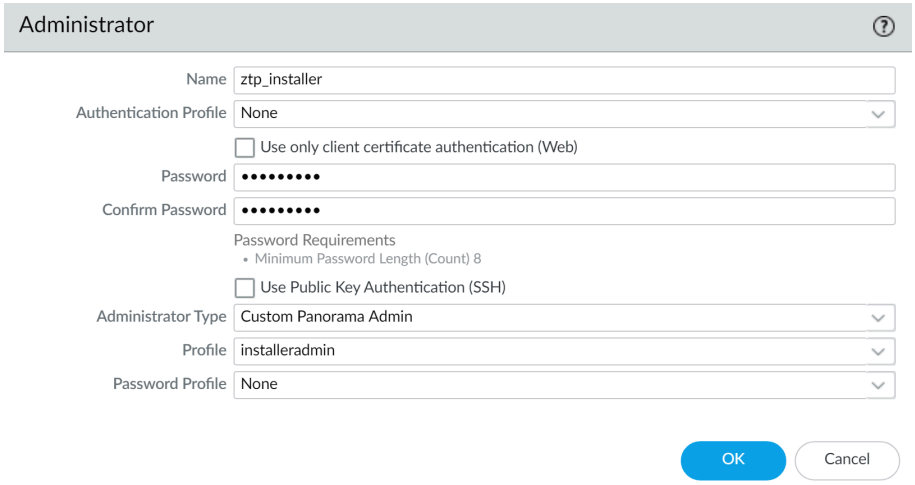
STEP 2 | **Panorama** > 관리자 역할을 선택한 다음 `installeradmin` 관리자 역할이 생성되었는지 확인합니다.

###는 Panorama에 ZTP 플러그인을 성공적으로 설치한 후 자동으로 생성됩니다.



STEP 3 | ZTP 설치 관리자 사용자를 구성합니다.

1. **Panorama** > 관리자를 선택한 다음 새 관리자 사용자를 추가합니다.
2. ZTP 설치 관리자 관리자를 설명하는 이름을 입력합니다.
3. 보안 암호 및 암호 확인을 입력합니다.
4. 관리자 유형으로 사용자 지정 **Panorama** 관리자를 선택합니다.
5. 프로파일에서 **installeradmin**을 선택합니다.
6. 확인을 클릭하여 구성 변경 사항을 저장합니다.



STEP 4 | 커밋 및 **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

Panorama에 ZTP 방화벽 추가

단일 ZTP 방화벽을 추가하거나 여러 ZTP 방화벽을 Panorama™ 관리 서버로 가져올 수 있습니다.

- Panorama에 ZTP 방화벽 추가
- 여러 ZTP 방화벽을 Panorama로 가져오기

Panorama에 ZTP 방화벽 추가

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• NGFW (Managed by Panorama)	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스 ❑ 클레임 키 ❑ 인증 코드

Panorama™ 관리 서버의 웹 인터페이스에 운용 관리자, Panorama 관리자 또는 ZTP 설치 관리자로 로그인하여 Panorama에 ZTP 방화벽을 추가합니다. ZTP 방화벽을 추가하려면 Palo Alto Networks에서 제공하는 방화벽 일련번호와 클레임 키를 입력한 다음 ZTP 서비스에 방화벽을 등록해야 합니다. 방화벽을 등록하면 고객 지원 포털에 있는 계정의 자산으로 방화벽을 주장하고 ZTP 서비스가 방화벽을 Panorama와 연결할 수 있습니다.

ZTP 방화벽을 Panorama에 성공적으로 추가하기 전에 동적 호스트 구성 프로토콜(DHCP) 서버가 네트워크에 배포되었는지 확인해야 합니다. ZTP 방화벽을 Panorama에 성공적으로 온보딩하려면 DHCP 서버가 필요합니다. ZTP 방화벽은 DHCP 서버 없이 온보딩을 용이하게 하기 위해 Palo Alto Networks ZTP 서비스에 연결할 수 없습니다.

필요한 모든 설치 및 설정 절차를 완료할 때까지 ZTP 방화벽의 전원을 켜지 마십시오.

- 필요한 모든 설치 및 설정 절차를 완료할 때까지 *ZTP* 방화벽의 전원을 켜지 마십시오. 이로 인해 *ZTP* 온보딩이 실패하므로 방화벽을 공장 기본 설정으로 재설정하여 *ZTP* 온보딩 프로세스를 다시 시작해야 합니다.

- 한 *Panorama*에서 다른 *Panorama*로 *ZTP*를 사용하여 *Panorama* 관리에 추가된 방화벽을 마이그레이션하는 것은 지원되지 않습니다.

  *ZTP*를 사용하여 *Panorama* 관리에 온보딩된 방화벽은 고가용성*(HA)* 구성을 지원하지 않습니다.

  HA 구성에서 *ZTP*를 구성하려면 방화벽에서 ZTP를 비활성화해야 합니다. *ZTP*를 비활성화한 후 방화벽을 관리형 디바이스로 추가하고 방화벽을 활성/수동 또는 활성/활성 *HA* 구성으로 설정합니다.

©2024 Palo Alto Networks, Inc.

*Panorama*에 *ZTP* 방화벽을 추가하는 동안 방화벽이 *Panorama*에 성공적으로 추가되는 것을 확인하기 전까지 *ZTP* 방화벽에서 커밋을 수행하지 마십시오. *ZTP* 방화벽에서 로컬 커밋을 수행하면 *ZTP* 기능이 비활성화되고 *Panorama*에 방화벽을 성공적으로 추가하지 못하게 됩니다.

- 11.1
- 11.2 이상

11.1

STEP 1 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에 ZTP 방화벽을 추가합니다.

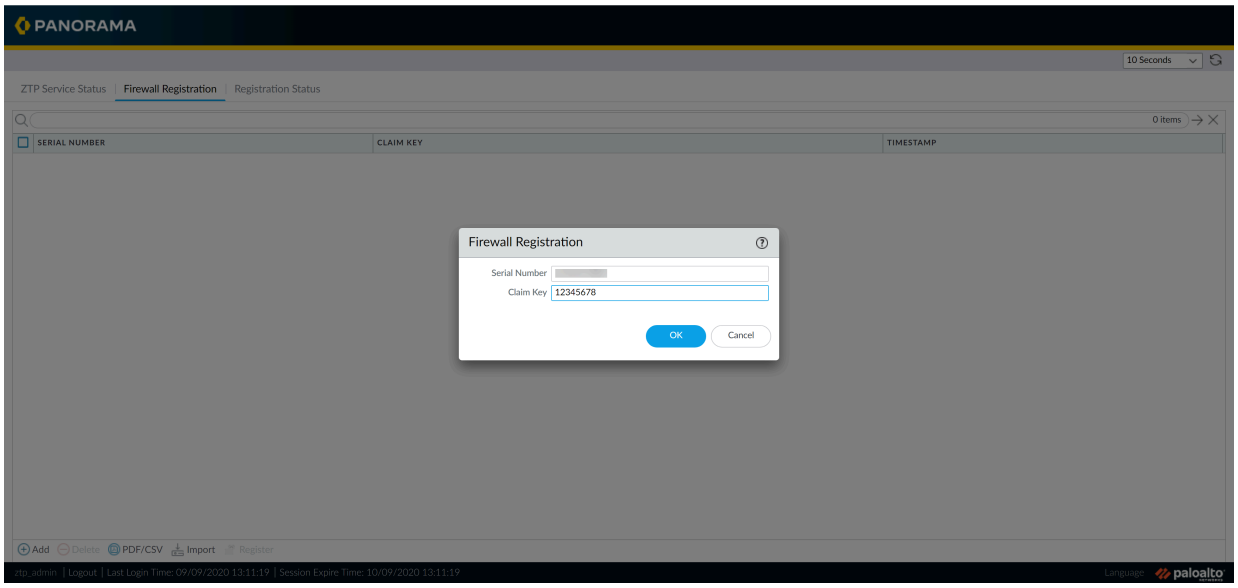
ZTP 방화벽을 *CSP*에 성공적으로 등록하고 정책 및 네트워크 구성을 푸시하려면 *Eth1/1* 인터페이스를 사용하여 *ZTP* 방화벽의 인터넷에 연결해야 합니다.

1. 방화벽 등록을 선택하고 새 ZTP 방화벽을 추가합니다.
2. ZTP 방화벽의 일련번호를 입력합니다.
3. Palo Alto Networks에서 제공한 ZTP 방화벽에 대한 클레임 키를 입력합니다.

   8자리 숫자 클레임 키는 Palo Alto Networks에서 받은 ZTP 방화벽 뒷면에 부착된 물리적 레이블에 인쇄되어 있습니다.



4. 확인을 클릭하여 구성 변경 사항을 저장합니다.



5. 새로 추가된 ZTP 방화벽을 선택하고 방화벽을 등록합니다.

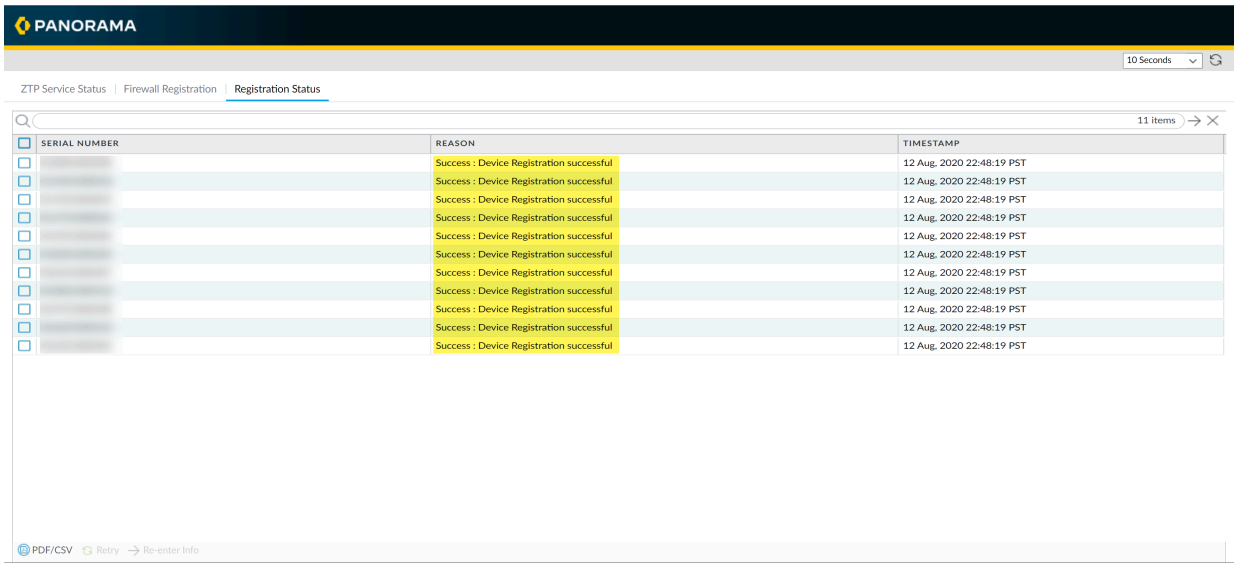
   메시지가 표시되면 예를 클릭하여 ZTP 방화벽 등록을 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 3 | 방화벽이 CSP에 성공적으로 등록되었는지 확인합니다.

디바이스 인증서를 성공적으로 얻으려면 방화벽이 *CSP*에 성공적으로 등록되어야 합니다.

1. 등록 상태를 선택하고 ZTP 방화벽이 CSP에 성공적으로 등록되었는지 확인합니다.



2. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하고 ZTP 방화벽이 관리형 방화벽으로 완전히 추가되었는지 확인합니다.

   ZTP 방화벽이 나열되어 있지만 ## ### 디바이스 상태가 있습니다.

   방화벽이 실수로 업그레이드 또는 다운그레이드하지 않도록 ***To SW Version*** 열이 올바른 *PAN-OS* 버전으로 구성되었는지 확인하십시오. *ZTP* 기능은 *PAN-OS 10.0.1* 이상의 버전에서만 지원됩니다. 또한 *PAN-OS* 버전은 *Panorama*에서 실행되는 *PAN-OS* 버전과 같거나 이전 버전이어야 합니다.

   자세한 내용은 ZTP 방화벽 업그레이드를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 필요한 ZTP 구성을 포함하는 디바이스 그룹 및 템플릿 스택에 ZTP 방화벽을 추가합니다.

방화벽이 푸시 정책 및 네트워크 구성에 ###으로 표시되도록 하려면 ZTP 방화벽을 디바이스 그룹 및 템플릿 스택(template stack)에 추가해야 합니다.

ZTP 템플릿이 연결된 *ZTP* 디바이스 그룹 및 템플릿 스택에 *ZTP* 방화벽을 유지해야 합니다. 이는 방화벽이 *Panorama*와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌릴 수 없도록 하는 데 필요합니다.

1. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
3. 이전 단계에서 추가하고 등록한 ZTP 방화벽을 선택하고 다시 연결합니다.
4. ZTP 디바이스 그룹 및 템플릿 스택**(template stack)**을 선택합니다.
5. ZTP 방화벽이 처음으로 Panorama에 성공적으로 연결되었을 때 디바이스 그룹 및 템플릿 스택(template stack) 구성을 자동으로 푸시하려면 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.
6. (선택 사항) 방화벽을 최신 PAN-OS 버전으로 자동 업그레이드하려면 **SW** 버전으로를 지정합니다.

   방화벽이 실수로 업그레이드 또는 다운그레이드하지 않도록 ***To SW Version*** 열이 올바른 *PAN-OS* 버전으로 구성되었는지 확인하십시오. *ZTP* 기능은 *PAN-OS 10.0.1* 이상의 버전에서만 지원됩니다. 또한 *PAN-OS* 버전은 *Panorama*에서 실행되는 *PAN-OS* 버전과 같거나 이전 버전이어야 합니다.

   자세한 내용은 ZTP 방화벽 업그레이드를 참조하십시오.
7. 커밋하고 **Panorama**에 커밋합니다.

STEP 5 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽의 전원이 켜질 때까지 기다립니다. Panorama에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 현재 ZTP 방화벽이 ##되었는지 확인합니다.

STEP 6 | 새로 온보딩된 방화벽 설정을 완료합니다.

1. 방화벽 웹 인터페이스에 로그인하고 지원 라이선스를 활성화합니다.
2. Panorama 웹 인터페이스에 로그인하고 관리형 방화벽에서 추가 라이선스를 활성화합니다.
3. 관리형 방화벽에 최신 동적 콘텐츠 업데이트를 설치합니다.
   1. 최신 버전으로 업데이트하려면 **Panorama** > 디바이스 배포 > 동적 업데이트를 선택하고 지금 확인을 선택합니다.
   2. 최신 동적 콘텐츠 릴리스 버전을 다운로드합니다.
   3. 새로 추가된 방화벽을 설치하고 선택합니다.

      메시지가 표시되면 확인을 클릭합니다.
4. (선택 사항) 필요에 따라 관리형 방화벽을 업그레이드합니다.

11.2 이상

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에 ZTP 방화벽을 추가합니다.

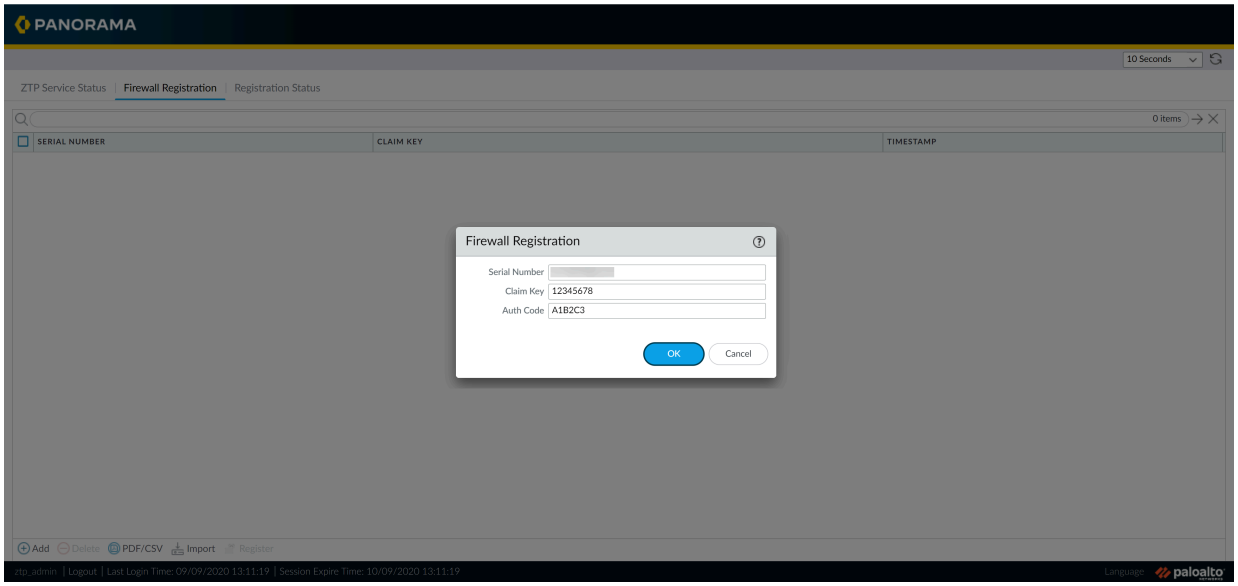
ZTP 방화벽을 *CSP*에 성공적으로 등록하고 정책 및 네트워크 구성을 푸시하려면 *Eth1/1* 인터페이스를 사용하여 *ZTP* 방화벽의 인터넷에 연결해야 합니다.

1. 방화벽 등록을 선택하고 새 ZTP 방화벽을 추가합니다.
2. ZTP 방화벽의 일련번호를 입력합니다.
3. Palo Alto Networks에서 제공한 ZTP 방화벽에 대한 클레임 키를 입력합니다.

   8자리 숫자 클레임 키는 Palo Alto Networks에서 받은 ZTP 방화벽 뒷면에 부착된 물리적 레이블에 인쇄되어 있습니다.



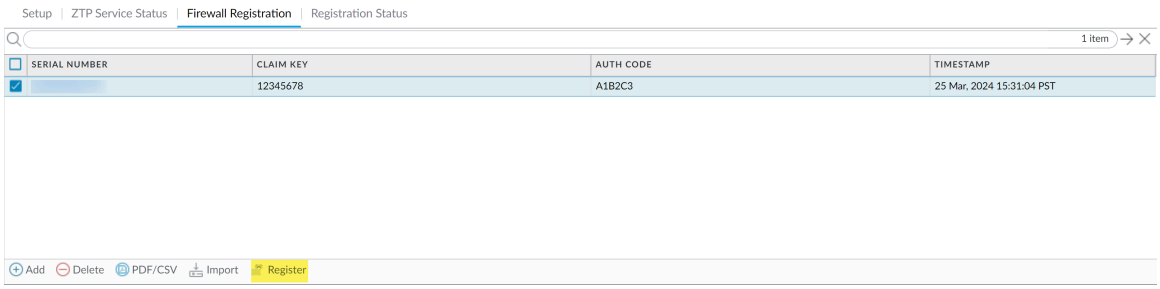
4. 처음 Panorama에 연결한 후 ZTP의 인증 코드를 입력하여 방화벽에서 라이선스를 활성화합니다.
5. 확인을 클릭하여 구성 변경 사항을 저장합니다.



6. 새로 추가된 ZTP 방화벽을 선택하고 방화벽을 등록합니다.

   메시지가 표시되면 예를 클릭하여 ZTP 방화벽 등록을 확인합니다.

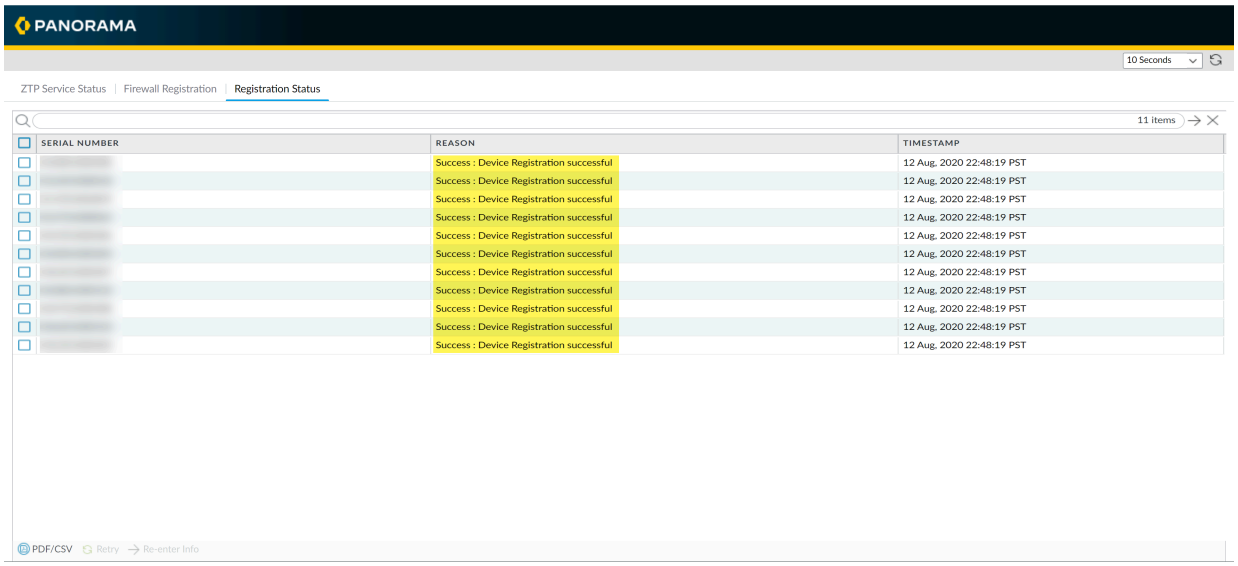
©2024 Palo Alto Networks, Inc.



STEP 3 | 방화벽이 CSP에 성공적으로 등록되었는지 확인합니다.

디바이스 인증서를 성공적으로 얻으려면 방화벽이 *CSP*에 성공적으로 등록되어야 합니다.

1. 등록 상태를 선택하고 ZTP 방화벽이 CSP에 성공적으로 등록되었는지 확인합니다.



2. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하고 ZTP 방화벽이 관리형 방화벽으로 완전히 추가되었는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 필요한 ZTP 구성을 포함하는 디바이스 그룹 및 템플릿 스택에 ZTP 방화벽을 추가합니다.

방화벽이 푸시 정책 및 네트워크 구성에 ###으로 표시되도록 하려면 ZTP 방화벽을 디바이스 그룹 및 템플릿 스택(template stack)에 추가해야 합니다.

ZTP 템플릿이 연결된 *ZTP* 디바이스 그룹 및 템플릿 스택에 *ZTP* 방화벽을 유지해야 합니다. 이는 방화벽이 *Panorama*와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌릴 수 없도록 하는 데 필요합니다.

1. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
3. 이전 단계에서 추가하고 등록한 ZTP 방화벽을 선택하고 다시 연결합니다.
4. ZTP 디바이스 그룹 및 템플릿 스택**(template stack)**을 선택합니다.
5. ZTP 방화벽이 처음으로 Panorama에 성공적으로 연결되었을 때 디바이스 그룹 및 템플릿 스택(template stack) 구성을 자동으로 푸시하려면 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.
6. (선택 사항) 방화벽을 최신 PAN-OS 버전으로 자동 업그레이드하려면 **SW** 버전으로를 지정합니다.

   방화벽이 실수로 업그레이드 또는 다운그레이드하지 않도록 ***To SW Version*** 열이 올바른 *PAN-OS* 버전으로 구성되었는지 확인하십시오. *ZTP* 기능은 *PAN-OS 10.0.1* 이상의 버전에서만 지원됩니다. 또한 *PAN-OS* 버전은 *Panorama*에서 실행되는 *PAN-OS* 버전과 같거나 이전 버전이어야 합니다.

   자세한 내용은 ZTP 방화벽 업그레이드를 참조하십시오.
7. 커밋하고 **Panorama**에 커밋합니다.

STEP 5 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽의 전원이 켜질 때까지 기다립니다. Panorama에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 현재 ZTP 방화벽이 ##되었는지 확인합니다.

여러 ZTP 방화벽을 Panorama로 가져오기

Panorama™ 관리 서버의 웹 인터페이스에 운용 관리자, Panorama 관리자 또는 ZTP 설치 관리자로 로그인하여 여러 ZTP 방화벽을 Panorama로 가져옵니다. 여러 ZTP 방화벽을 가져오려면 Palo Alto Networks에서 제공한 ZTP 방화벽 일련번호 및 해당 클레임 키의 CSV 파일을 불러온 다음 ZTP 서비스에 방화벽을 등록해야 합니다. 방화벽을 등록하면 방화벽이 고객 지원 포털에서 계정의 자산으로 요구되고 ZTP 서비스가 방화벽을 Panorama와 연결할 수 있습니다.

ZTP 방화벽을 Panorama에 성공적으로 추가하기 전에 동적 호스트 구성 프로토콜(DHCP) 서버가 네트워크에 배포되었는지 확인해야 합니다. ZTP 방화벽을 Panorama에 성공적으로 온보딩하려면 DHCP 서버가 필요합니다. ZTP 방화벽은 DHCP 서버 없이 온보딩을 용이하게 하기 위해 Palo Alto Networks ZTP 서비스에 연결할 수 없습니다.

필요한 모든 설치 및 설정 절차를 완료할 때까지 *ZTP* 방화벽의 전원을 켜지 마십시오. 이로 인해 *ZTP* 온보딩이 실패하므로 방화벽을 공장 기본 설정으로 재설정하여 *ZTP* 온보딩 프로세스를 다시 시작해야 합니다.

 ©2024 Palo Alto Networks, Inc.

한 *Panorama*에서 다른 *Panorama*로 *ZTP*를 사용하여 *Panorama* 관리에 추가된 방화벽을 마이그레이션하는 것은 지원되지 않습니다.

*ZTP*를 사용하여 *Panorama* 관리에 온보딩된 방화벽은 고가용성*(HA)* 구성을 지원하지 않습니다.

HA 구성에서 *ZTP*를 구성하려면 방화벽에서 ZTP를 비활성화해야 합니다. *ZTP*를 비활성화한 후 방화벽을 관리형 디바이스로 추가하고 방화벽을 활성/수동 또는 활성/활성 *HA* 구성으로 설정합니다.

*Panorama*에 *ZTP* 방화벽을 추가하는 동안 방화벽이 *Panorama*에 성공적으로 추가되는 것을 확인하기 전까지 *ZTP* 방화벽에서 커밋을 수행하지 마십시오. *ZTP* 방화벽에서 로컬 커밋을 수행하면 *ZTP* 기능이 비활성화되고 *Panorama*에 방화벽을 성공적으로 추가하지 못하게 됩니다.

- 11.1
- 11.2 이상

11.1

STEP 1 | ZTP 방화벽에 대한 일련 번호와 클레임 키를 수집합니다.

8자리 숫자 클레임 키는 Palo Alto Networks에서 받은 ZTP 방화벽 뒷면에 부착된 물리적 레이블에 인쇄되어 있습니다.



STEP 2 | Panorama 웹 인터페이스에 로그인.

STEP 3 | **Panorama** > **Zero Touch Provisioning** > 방화벽 등록 > **PDF/CSV**를 선택하고 빈 ZTP 가져오기 파일을 `.csv` 형식으로 내보냅니다.

STEP 4 | ZTP 방화벽 일련 번호 및 클레임 키가 포함된 CSV 파일을 만듭니다. 첫 번째 열에는 일련번호가 포함되어야 하고, 두 번째 열에는 해당 방화벽에 대한 해당 클레임 키가 포함되어야 하며, 세 번째 열에는 방화벽 라이선스를 활성화하기 위한 인증 키가 포함되어야 합니다. 참고로 다음 예를 참조하십시오.

	A	B
1	Serial Number	Claim Key
2	abcd1234	123456789
3	xyz7890	987654321

©2024 Palo Alto Networks, Inc.

STEP 5 | ZTP 방화벽을 Panorama로 가져옵니다.

ZTP 방화벽을 *CSP*에 성공적으로 등록하고 정책 및 네트워크 구성을 푸시하려면 *ZTP* 방화벽의 *Eth1/1* 인터페이스를 연결해야 합니다.

1. ZTP 설치 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > **Zero Touch Provisioning** > 방화벽 등록을 선택한 다음 ZTP 방화벽을 가져옵니다.
3. TP 방화벽 정보가 포함된 CSV 파일을 찾아 선택한 다음 확인을 클릭합니다.
4. 새로 추가된 ZTP 방화벽을 선택하고 방화벽을 등록합니다.

   메시지가 표시되면 예를 클릭하여 ZTP 방화벽 등록을 확인합니다.

STEP 6 | 방화벽이 ZTP 서비스에 성공적으로 등록되었는지 확인합니다.

1. 등록 상태를 선택한 다음 ZTP 방화벽이 ZTP 서비스에 성공적으로 등록되었는지 확인합니다.
2. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하고 ZTP 방화벽이 관리형 방화벽으로 성공적으로 추가되었는지 확인합니다.

STEP 7 | 필요한 ZTP 구성을 포함하는 디바이스 그룹 및 템플릿 스택(template stack)에 ZTP 방화벽을 추가합니다.

방화벽이 푸시 정책 및 네트워크 구성에 ###으로 표시되도록 하려면 ZTP 방화벽을 디바이스 그룹 및 템플릿 스택(template stack)에 추가해야 합니다.

ZTP 템플릿이 연결된 *ZTP* 디바이스 그룹 및 템플릿 스택*(template stack)*에 *ZTP* 방화벽을 유지해야 합니다. 이는 방화벽이 *Panorama*와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌려지지 않도록 방지하는 데 필요합니다.

1. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
3. 이전 단계에서 추가하고 등록한 ZTP 방화벽을 선택하고 다시 연결합니다.
4. ZTP 디바이스 그룹 및 템플릿 스택**(template stack)**을 선택합니다.
5. ZTP 방화벽이 처음으로 Panorama에 성공적으로 연결되었을 때 디바이스 그룹 및 템플릿 스택(template stack) 구성을 자동으로 푸시하려면 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.
6. (선택 사항) 방화벽을 최신 PAN-OS 버전으로 자동 업그레이드하려면 **SW** 버전으로를 지정합니다.

   방화벽이 실수로 업그레이드 또는 다운그레이드하지 않도록 ***To SW Version*** 열이 올바른 *PAN-OS* 버전으로 구성되었는지 확인하십시오. *ZTP* 기능은 *PAN-OS 10.0.1* 이상의 버전에서만 지원됩니다. 또한 *PAN-OS* 버전은 *Panorama*에서 실행되는 *PAN-OS* 버전과 같거나 이전 버전이어야 합니다.

   자세한 내용은 ZTP 방화벽 업그레이드를 참조하십시오.
7. 커밋하고 **Panorama**에 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽의 전원이 켜질 때까지 기다립니다. Panorama에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 현재 ZTP 방화벽이 ##되었는지 확인합니다.

STEP 9 | 새로 온보딩된 방화벽 설정을 완료합니다.

1. 방화벽 웹 인터페이스에 로그인하고 지원 라이선스를 활성화합니다.

   Panorama 관리에 추가한 각 관리형 방화벽에 대해 로컬에서 지원 라이선스를 활성화해야 합니다.
2. Panorama 웹 인터페이스에 로그인하고 관리형 방화벽에서 추가 라이선스를 활성화합니다.
3. 관리형 방화벽에 최신 동적 콘텐츠 업데이트를 설치합니다.
   1. 최신 버전으로 업데이트하려면 **Panorama** > 디바이스 배포 > 동적 업데이트를 선택하고 지금 확인을 선택합니다.
   2. 최신 동적 콘텐츠 릴리스 버전을 다운로드합니다.
   3. 새로 추가된 방화벽을 설치하고 선택합니다.

      메시지가 표시되면 확인을 클릭합니다.
4. (선택 사항) 필요에 따라 관리형 방화벽을 업그레이드합니다.

11.2 이상

STEP 1 | ZTP 방화벽에 대한 일련번호, 클레임 키, 인증 코드를 수집합니다.

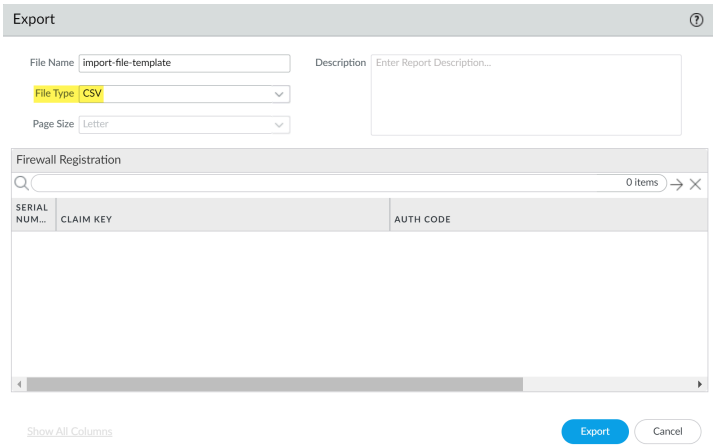
8자리 숫자 클레임 키는 Palo Alto Networks에서 받은 ZTP 방화벽 뒷면에 부착된 물리적 레이블에 인쇄되어 있습니다.



STEP 2 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | **Panorama** > **Zero Touch Provisioning** > 방화벽 등록 > **PDF/CSV**를 선택하고 빈 ZTP 가져오기 파일을 `.csv` 형식으로 내보냅니다.



STEP 4 | ZTP 방화벽 일련 번호 및 클레임 키가 포함된 CSV 파일을 만듭니다. 첫 번째 열에는 일련번호가 포함되어야 하고 두 번째 열에는 해당 방화벽에 대한 해당 클레임 키가 포함되어야 합니다. 참고로 다음 예를 참조하십시오.

A	B	C
Serial Number	Claim Key	Auth Code
abcd1234	123456789	A1B2C3
efgh5678	987654321	D1E2F3

STEP 5 | ZTP 방화벽을 Panorama로 가져옵니다.

ZTP 방화벽을 *CSP*에 성공적으로 등록하고 정책 및 네트워크 구성을 푸시하려면 *ZTP* 방화벽의 *Eth1/1* 인터페이스를 연결해야 합니다.

1. ZTP 설치 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > **Zero Touch Provisioning** > 방화벽 등록을 선택한 다음 ZTP 방화벽을 가져옵니다.
3. TP 방화벽 정보가 포함된 CSV 파일을 찾아 선택한 다음 확인을 클릭합니다.
4. 새로 추가된 ZTP 방화벽을 선택한 다음 방화벽을 등록합니다.

   메시지가 표시되면 예를 클릭하여 ZTP 방화벽 등록을 확인합니다.

STEP 6 | 방화벽이 ZTP 서비스에 성공적으로 등록되었는지 확인합니다.

1. 등록 상태를 선택한 다음 ZTP 방화벽이 ZTP 서비스에 성공적으로 등록되었는지 확인합니다.
2. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하고 ZTP 방화벽이 관리형 방화벽으로 성공적으로 추가되었는지 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 7 | 필요한 ZTP 구성을 포함하는 디바이스 그룹 및 템플릿 스택(template stack)에 ZTP 방화벽을 추가합니다.

방화벽이 푸시 정책 및 네트워크 구성에 ###으로 표시되도록 하려면 ZTP 방화벽을 디바이스 그룹 및 템플릿 스택(template stack)에 추가해야 합니다.

ZTP 템플릿이 연결된 *ZTP* 디바이스 그룹 및 템플릿 스택*(template stack)*에 *ZTP* 방화벽을 유지해야 합니다. 이는 방화벽이 *Panorama*와의 연결을 유지하고 방화벽에서 의도하지 않은 구성이 되돌려지지 않도록 방지하는 데 필요합니다.

1. 관리자 자격 증명을 사용한 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
3. 이전 단계에서 추가하고 등록한 ZTP 방화벽을 선택하고 다시 연결합니다.
4. ZTP 디바이스 그룹 및 템플릿 스택**(template stack)**을 선택합니다.
5. ZTP 방화벽이 처음으로 Panorama에 성공적으로 연결되었을 때 디바이스 그룹 및 템플릿 스택(template stack) 구성을 자동으로 푸시하려면 첫 번째 연결 시 자동 푸시를 선택(활성화)합니다.
6. (선택 사항) 방화벽을 최신 PAN-OS 버전으로 자동 업그레이드하려면 **SW** 버전으로를 지정합니다.

   방화벽이 실수로 업그레이드 또는 다운그레이드하지 않도록 ***To SW Version*** 열이 올바른 *PAN-OS* 버전으로 구성되었는지 확인하십시오. *ZTP* 기능은 *PAN-OS 10.0.1* 이상의 버전에서만 지원됩니다. 또한 *PAN-OS* 버전은 *Panorama*에서 실행되는 *PAN-OS* 버전과 같거나 이전 버전이어야 합니다.

   자세한 내용은 ZTP 방화벽 업그레이드를 참조하십시오.
7. 커밋하고 **Panorama**에 커밋합니다.

STEP 8 | ZTP 방화벽의 전원을 켭니다.

ZTP 방화벽의 전원이 켜질 때까지 기다립니다. Panorama에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 현재 ZTP 방화벽이 ##되었는지 확인합니다.

ZTP 작업에 CLI 사용

다음 CLI 명령을 사용하여 ZTP(Zero Touch Provisioning) 작업을 수행하고 ZTP 서비스 상태를 봅니다.

원하는 경우...	사용...
방화벽 **CLI**에서 방화벽 관리	
ZTP 서비스에 대한 연결 상태를 표시합니다.	`> show system ZTP status`
Panorama 관리 서버에 대한 연결 상태를 표시합니다.	`> show panorama status`

 ©2024 Palo Alto Networks, Inc.

원하는 경우...	사용...
ZTP 모델 번호와 방화벽 시스템 정보를 표시합니다.	`> show system info`
방화벽에서 ZTP 상태 시스템을 활성화합니다. PA-5400, PA-400, PA-410, PA-1400 및 PA-3400 전용입니다.	`> set system ztp enable` *ZTP* 상태 머신을 다시 활성화하면 소프트 팩토리 재설정이 시작되어 기존 방화벽 구성이 삭제됩니다.
방화벽에서 ZTP 상태 시스템을 비활성화합니다. *ZTP* 상태 머신을 비활성화하면 소프트 팩토리 재설정이 시작되어 기존 방화벽 구성이 삭제됩니다.	`> request disable-ztp` PA-220-ZTP, PA-220R-ZTP, PA-800-ZTP, PA-850-ZTP, PA-3220-ZTP, PA-3250-ZTP 및 PA-3260-ZTP 전용 *CLI*에서 비활성화된 후에는 방화벽에서 *ZTP* 상태 시스템을 다시 활성화할 수 없습니다. 다시 활성화하려면 방화벽을 공장 기본 설정으로 재설정해야 합니다.
	`> set system ztp disable` PA-5400, PA-400, PA-410, PA-1400 및 PA-3400 전용입니다.
Panorama에서 **ZTP** 방화벽 등록, 구성 및 관리	
Eth1/1 인터페이스에서 ZTP 서비스를 사용하여 Panorama와 관리 방화벽을 연결하는 데 필요한 구성이 포함된 디바이스 그룹 또는 템플릿을 생성합니다.	`> request plugins ztp create dgroup-template device-group <device group name>` `> request plugins ztp create dgroup-template template <template name>`

©2024 Palo Alto Networks, Inc.

원하는 경우...	사용...
ZTP 서비스에 나중에 등록할 수 있도록 방화벽 목록에 ZTP 방화벽을 추가합니다.	`> request plugins ztp firewall-add <serial number> claim-key <claim key>`
ZTP 서비스에 대한 향후 등록을 위해 방화벽 목록에 이미 추가된 ZTP 방화벽의 일련번호를 수정합니다.	`> request plugins ztp firewall-add-modify firewall <old serial number> claim-key <claim key> new-serial <new serial number>`
ZTP 서비스에 나중에 등록할 수 있도록 방화벽 목록에서 ZTP 방화벽을 삭제합니다.	`> request plugins ztp firewall-delete firewall <serial number>`
ZTP 서비스에 향후 재등록을 위해 방화벽 목록에 ZTP 방화벽을 추가합니다. ZTP 방화벽이 처음에 ZTP 서비스 등록에 실패하고 필요할 때 이 명령을 사용합니다.	`> request plugins ztp firewall-re-enter-info firewall <serial number> claim-key <claim key>`
Panorama™ 관리 서버를 ZTP 서비스에 등록합니다.	`> request plugins ztp panorama-registration`
ZTP 서비스에 ZTP 방화벽을 등록합니다.	`> request plugins ztp firewall-registration firewall <serial number> claim-key <claim key>`
ZTP 서비스에 ZTP 방화벽을 다시 등록하십시오. 이 명령을 사용하여 ZTP 서비스에 초기 등록에 실패한 ZTP 방화벽에 대한 재등록 프로세스를 시작합니다.	`> request plugins ztp firewall-register-retry firewall <serial number> claim-key <claim key>`
ZTP 방화벽 일련번호를 가져오고 키 정보를 요청합니다. 지정된 파일은 CSV 형식이어야 합니다.	`> request plugins ztp ztp-add-import import-path <file path>`
Panorama에서 **ZTP** 방화벽 정보 및 **ZTP** 서비스 상태 보기	
ZTP 서비스에서 Panorama에 등록된 ZTP 방화벽 목록을 검색합니다.	`> request plugins ztp ztp-service-info`

©2024 Palo Alto Networks, Inc.

원하는 경우...	사용...
	다음 세부 정보가 표시됩니다. • `first-firewall-connect-time` - ZTP 방화벽이 ZTP 서비스에 처음 연결된 시간의 타임스탬프입니다. • `last-firewall-connect-time` - ZTP 방화벽이 ZTP 서비스에 마지막으로 연결된 시간의 타임스탬프입니다. • `registration-time` - ZTP 방화벽이 ZTP 서비스에 등록된 시간의 타임스탬프입니다. • `isZTPFirewall` - 방화벽이 ZTP 방화벽인지의 여부입니다. • `created_by` - ZTP 방화벽을 추가한 관리자입니다. • `IP ##` - ZTP 방화벽의 IP 주소입니다.
ZTP 서비스에 등록할 방화벽 목록에서 ZTP 방화벽 목록을 봅니다.	`> show plugins ztp device-add-list`
ZTP 방화벽의 등록 상태를 봅니다.	`> show plugins ztp device-reg-status`
ZTP 방화벽에 대한 ZTP 서비스 동기화 상태를 봅니다.	`> request plugins ztp ztp-sync-status`
전체 관리 평면 ZTP 연결 기록을 표시합니다. 이는 ZTP 서비스 연결 문제를 해결하는 데 유용합니다.	`> tail follow yes mp-log ms.log`

ZTP 플러그인 제거

Panorama™ 관리 서버에서 ZTP 구성을 제거하고 ZTP 플러그인을 제거하는 절차를 따르십시오. Panorama가 고가용성(HA) 구성에 있는 경우 두 Panorama HA 피어에서 이 단계를 반복합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

©2024 Palo Alto Networks, Inc.

STEP 2 | ZTP 설치 관리자 계정을 삭제합니다.

1. **Panorama** > 관리자를 선택한 다음 이전에 구성한 ZTP 설치 관리자 계정을 선택합니다.
2. ZTP 설치 관리자 계정을 삭제합니다.
3. **Panorama** > 관리자를 선택한 다음 `installeradmin` 관리자 역할을 선택합니다.
4. `installeradmin` 관리자 역할을 삭제합니다.
5. 커밋 및 **Panorama**에 커밋을 선택합니다.

STEP 3 | ZTP 플러그인 제거

1. **Panorama** > 플러그인을 선택한 다음 Panorama에 설치된 ZTP 플러그인으로 이동합니다.
2. 작업 열에서 구성 제거를 통해 Panorama에서 ZTP 관련 구성을 삭제합니다.
3. Panorama에서 ZTP 구성 제거를 확인하는 메시지가 표시되면 확인을 클릭합니다.
4. 커밋 및 **Panorama**에 커밋을 선택합니다.
5. ZTP 플러그인을 제거합니다.
6. Panorama에서 ZTP 플러그인을 제거할지 묻는 메시지가 표시되면 확인을 클릭합니다.

©2024 Palo Alto Networks, Inc.

디바이스 그룹 관리

- 디바이스 그룹 추가
- 디바이스 그룹 계층 생성
- 공유 또는 디바이스 그룹 정책에서 사용할 개체 생성
- 상속된 개체 값으로 되돌리기
- 미사용 공유 객체 관리
- 상속된 개체의 우선 순위 관리
- 정책 규칙 또는 다른 디바이스 그룹으로 이동 또는 복제
- 방화벽의 하위 집합에 정책 규칙 푸시
- Multi-VSYS 방화벽으로 디바이스 그룹 푸시
- 규칙 계층 구조 관리

디바이스 그룹 추가

방화벽을 추가한 후(관리되는 디바이스로 방화벽 추가 참조) 다음과 같이 방화벽을 디바이스 그룹(최대 1,024개)에 그룹화할 수 있습니다. Panorama가 동일한 정책 규칙 및 개체를 해당 방화벽에 푸시할 수 있도록 활성-수동 HA(고가용성) 구성의 두 방화벽을 동일한 디바이스 그룹에 할당해야 합니다. PAN-OS는 HA 피어 간에 푸시된 규칙을 동기화하지 않습니다. 조직의 다양한 관리 수준에서 규칙과 개체를 관리하려면, 디바이스 그룹 계층 생성.

STEP 1 | **Panorama** > 디바이스 그룹을 선택하고 추가를 클릭합니다.

STEP 2 | 디바이스 그룹을 식별하기 위해 고유한 이름 및 설명을 입력합니다.

STEP 3 | 디바이스 섹션에서 확인란을 선택하여 그룹에 방화벽을 할당합니다. 긴 방화벽 목록을 검색하려면 필터를 사용합니다.

> 방화벽은 하나의 디바이스 그룹에만 할당할 수 있습니다. 방화벽의 각 가상 시스템을 다른 디바이스 그룹에 할당할 수 있습니다.

STEP 4 | 참조 템플릿 섹션에서 디바이스 그룹 구성에서 참조하는 개체가 있는 템플릿 또는 템플릿 스택을 추가합니다.

템플릿 또는 템플릿 스택(template stack)을 디바이스 그룹에 성공적으로 연결하려면 적절한 템플릿 또는 템플릿 스택(template stack) 참조를 디바이스 그룹에 할당해야 합니다. 이를 통해 템플릿 스택(template stack)에 관련없는 디바이스를 추가하지 않고도 템플릿 또는 템플릿 스택(template stack)에 구성된 객체를 참조할 수 있습니다.

디바이스 그룹 구성이 템플릿 또는 템플릿 스택(template stack)에 구성된 개체를 참조하지 않는 경우 이 단계를 건너뜁니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (선택 사항) HA 피어인 방화벽에 대해 그룹 **HA** 피어를 선택합니다.

관리되는 방화벽 HA 피어가 동일한 디바이스 그룹에 있는 경우에만 그룹화할 수 있습니다.

수동 또는 활성 보조 피어의 방화벽 이름은 괄호 안에 있습니다. *HA* 피어 그룹화는 시각적 변경이며 구성 변경이 발생하지 않습니다.

STEP 6 | 디바이스 그룹 계층에서 생성하고 있는 디바이스 그룹 바로 위에 있는 상위 디바이스 그룹(기본값은 공유)을 선택합니다.

STEP 7 | 정책 규칙이 사용자 및 그룹을 참조하는 경우 마스터 방화벽을 할당합니다.

이것은 Panorama가 사용자 이름 및 사용자 그룹 정보를 수집하는 디바이스 그룹의 유일한 방화벽입니다.

STEP 8 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 9 | 커밋 > 커밋 및 푸시를 선택한 다음, Panorama 구성 및 추가한 디바이스 그룹에 대한 변경 사항을 커밋 및 푸시합니다.

디바이스 그룹 계층 생성

STEP 1 | 디바이스 그룹 계층을 계획합니다.

1. 디바이스 그룹 수준과 각 디바이스 그룹 및 공유 위치에 할당할 방화벽 및 가상 시스템을 결정합니다. 하나의 방화벽 또는 가상 시스템(vsys)을 하나의 디바이스 그룹에만 할당할 수 있습니다. 디바이스 그룹이 하위 수준 디바이스 그룹의 조직 컨테이너일 경우 여기에 방화벽을 할당할 필요가 없습니다.
2. 해당 할당이 계획된 계층에 맞지 않는 경우 기존 디바이스 그룹에서 방화벽 또는 vsys 할당을 제거합니다.
   1. **Panorama** > 디바이스 그룹을 선택한 다음 디바이스 그룹을 선택합니다.
   2. 디바이스 섹션에서 제거할 방화벽 및 가상 시스템의 확인란을 선택 취소하고 확인을 클릭합니다.
3. 필요한 경우 디바이스 그룹에 할당할 방화벽을 더 추가합니다. 관리형 디바이스로 방화벽 추가를 참조하십시오.
4. 여러 Panorama 플러그인을 사용하여 엔드포인트 모니터링을 수행하는 경우 특정 하이퍼바이저에 배포된 방화벽이 포함된 디바이스 그룹은 다른 하이퍼바이저에 배포된 방화벽이 포함된 디바이스 그룹의 하위 또는 상위 그룹이 될 수 없습니다. 자세한 내용은디바이스 그룹 계층을 참조하십시오.

STEP 2 | 각 최상위 디바이스 그룹에 대해 디바이스 그룹을 추가합니다.

1. **Panorama** > 디바이스 그룹 페이지에서 추가를 클릭하고 이름을 입력하여 디바이스 그룹을 식별합니다.
2. 디바이스 섹션에서 확인란을 선택하여 디바이스 그룹에 방화벽 및 가상 시스템을 할당합니다.
3. 상위 디바이스 그룹 옵션을 공유(기본값)로 두고 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 각 하위 수준 디바이스 그룹에 대해 디바이스 그룹을 추가합니다.

- 각 하위 수준의 새 디바이스 그룹에 대해 이전 단계를 반복하되 상위 디바이스 그룹을 상위 수준의 디바이스 그룹으로 설정합니다.
- 각 기존 디바이스 그룹에 대해 디바이스 그룹 페이지에서 편집할 디바이스 그룹을 선택한 다음 상위 디바이스 그룹을 선택한 다음 확인을 클릭합니다.



디바이스 그룹을 다른 상위로 이동하면 모든 하위 디바이스 그룹과 함께 모든 방화벽, 정책 규칙 및 디바이스 그룹 및 해당 하위 항목과 연결된 개체가 함께 이동합니다. 새 부모가 다른 액세스 도메인에 있는 경우 이동된 디바이스 그룹은 더 이상 원래 액세스 도메인의 구성원이 아닙니다. 새 액세스 도메인에 상위 디바이스 그룹에 대한 읽기-쓰기 액세스 권한이 있는 경우 이동된 디바이스 그룹에 대한 읽기-쓰기 액세스 권한도 갖게 됩니다. 새 액세스 도메인에 상위에 대한 읽기 전용 액세스 권한이 있는 경우 이동된 디바이스 그룹에 대한 액세스 권한이 없습니다. 디바이스 그룹에 대한 액세스를 재구성하려면 액세스 도메인 구성을 참조하십시오.

STEP 4 | 디바이스 그룹 계층 구조의 상속을 설명하기 위해 필요에 따라 개체 및 정책 규칙을 구성, 이동 및 복제합니다.

- 공유 또는 디바이스 그룹 정책에서 사용할 개체를 만들거나 기존 개체를 편집합니다.

개체는 해당 위치, 즉 개체가 할당된 디바이스 그룹에서만 편집할 수 있습니다. 하위 디바이스 그룹은 해당 위치에서 개체의 읽기 전용 인스턴스를 상속합니다. 그러나 상속된 개체 값 재정의 단계를 선택적으로 볼 수 있습니다.

- 정책을 만들거나 편집합니다.
- 정책 규칙 또는 개체를 다른 디바이스 그룹으로 이동하거나 복제합니다.

STEP 5 | 상속된 개체 값을 재정의합니다.

특정 디바이스 그룹의 개체 값이 상위 디바이스 그룹에서 상속된 값과 달라야 하는 경우에만 적용할 수 있습니다.

개체를 재정의한 후 하위 디바이스 그룹에서 다시 재정의할 수 있습니다. 그러나 공유 또는 사전 정의된(기본) 개체를 재정의할 수 없습니다.

개체 탭에서 상속된 개체는 이름 열에 녹색 아이콘이 있고 위치 열에는 상위 디바이스 그룹이 표시됩니다.

1. 개체 탭에서 개체 유형(예: 개체 > 주소)을 선택합니다.
2. 재정의 인스턴스를 가질 디바이스 그룹을 선택합니다.
3. 개체를 선택하고 재정의를 클릭합니다.
4. 값을 편집합니다. 이름 또는 공유 설정은 편집할 수 없습니다.
5. 확인을 클릭합니다. 이름 열에는 개체가 재정의되었음을 나타내는 노란색-중복-녹색 아이콘이 표시됩니다.



필요한 경우 나중에 상속된 개체 값으로 되돌릴 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 변경 사항을 저장하고 커밋합니다.

*Panorama*에 커밋하고 계층 구조를 변경한 후 디바이스 그룹에 푸시합니다.

템플릿이 디바이스 그룹의 개체(예: 주소를 참조하는 인터페이스)를 참조하고 템플릿에 할당된 방화벽이 계층 구조 변경으로 인해 해당 디바이스 그룹에 더 이상 할당되지 않은 경우에도 템플릿에 변경 사항을 푸시해야 합니다.

커밋 > 커밋 및 푸시를 선택한 다음 Panorama 구성 및 추가하거나 변경한 디바이스 그룹에 대한 변경 사항을 커밋 및 푸시합니다.

공유 또는 디바이스 그룹 정책에서 사용할 개체 생성

공유 위치에 있는 모든 정책 규칙이나 개체와 동일한 디바이스 그룹 또는 해당 디바이스 그룹의 하위 항목에서 개체를 사용할 수 있습니다(자세한 내용은 디바이스 그룹 개체 참조).

공유 디바이스 그룹 개체는 특정 디바이스 그룹에서 보고 참조할 수 있습니다. 한 디바이스 그룹에서 공유 디바이스 그룹 개체의 이름을 변경하면 모든 디바이스 그룹에서 공유 개체의 이름이 변경됩니다. 여기에는 정책 규칙과 같이 공유 개체가 참조하는 모든 구성이 포함됩니다. 공유 디바이스 그룹 개체의 이름을 변경하면 관리되는 방화벽에 대한 구성 푸시가 실패할 수 있습니다.

예를 들어 ObjectA라는 공유 개체를 만들고 ObjectA가 참조되는 DG1 디바이스 그룹에 보안 정책 규칙을 만듭니다. 이 구성은 관리형 방화벽으로 푸시됩니다. 나중에 DG1 디바이스 그룹에서 ObjectA의 이름을 ObjectB로 변경하고 구성을 관리되는 방화벽으로 푸시하려고 합니다. 관리되는 방화벽에 구성의 일부로 ObjectA라는 이름의 공유 개체가 있고 해당 구성 개체의 이름이 같을 것으로 예상하기 때문에 이 푸시는 실패합니다.

정책에서 동적 주소 그룹 사용을 참조하여 네트워크 변경에 자동으로 적응하는 정책을 생성하기 위한 목적으로 동적 주소 그룹을 활용하려는 경우 *Panorama*에서 지원되는 등록된 *IP* 주소 수를 확인하십시오.

©2024 Palo Alto Networks, Inc.

- 공유 개체를 생성합니다.

  이 예제에서는 경고를 트리거하려는 URL 필터링 카테고리에 대한 공유 개체를 추가합니다.

  1. 개체 > 보안 프로파일 > **URL** 필터링 탭을 선택한 다음 추가를 클릭합니다.

     개체 탭은 하나 이상의 디바이스 그룹 추가을(를) 수행한 후에만 나타납니다.
  2. 이름 및 설명을 입력합니다.
  3. 공유를 선택합니다.
  4. 기본값 사용 해제 옵션은 기본적으로 지워지므로 모든 디바이스 그룹에서 개체의 상속된 인스턴스를 재정의할 수 있습니다. 개체에 대한 재정의를 사용하지 않도록 설정하려면 확인란을 선택합니다.
  5. 카테고리 탭에서 알림을 원하는 모든 카테고리를 선택합니다.
  6. 작업 열에서 경고를 선택합니다.
  7. 확인을 클릭하여 개체에 변경 내용을 저장합니다.
  8. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

- 디바이스 그룹 개체를 생성합니다.

  이 예제에서는 네트워크의 특정 웹 서버에 대한 주소 개체를 추가합니다.

  1. 개체 > 주소를 선택한 다음 개체를 사용할 디바이스 그룹을 선택합니다.
  2. 추가를 클릭하고 이름을 입력하여 개체를 식별합니다.
  3. 공유 옵션을 지워 두어야 합니다.
  4. 기본으로 제거된 재정의 해제 옵션은 선택한 디바이스 그룹의 하위 항목인 디바이스 그룹에서 개체의 상속된 인스턴스를 재정의할 수 있습니다. 개체에 대한 재정의를 사용하지 않도록 설정하려면 재정의 비활성화 옵션을 선택합니다.
  5. 주소 개체 유형과 연결된 값을 선택합니다. 예를 들어 **IP** 범위를 선택한 다음 웹 서버에 대한 IP 주소 범위를 입력합니다.
  6. 확인을 클릭하여 개체에 변경 내용을 저장합니다.
  7. 커밋 > 커밋 및 푸시를 선택한 다음 변경 내용을 Panorama 구성및 개체를 추가한 디바이스 그룹으로 커밋하고 푸시합니다.

     방화벽에서 바이러스 백신 라이선스를 활성화하면 사전 정의된 *IP* 목록 목록이 방화벽에 자동으로 추가됩니다. 따라서 *Panorama*에서 푸시할 수 있는 개별 주소 개체, 동적 그룹, 외부 *IP* 목록, 사전 정의된 *IP* 블록 목록 및 외부 사전 정의된 *IP* 목록의 총 수가 줄어듭니다.

 ©2024 Palo Alto Networks, Inc.

- Panorama에서 공유 된 개체 및 디바이스 그룹 개체를 봅니다.

  개체 탭의 페이지에서 위치 열은 개체가 공유되는지 또는 디바이스 그룹에 특정하는지의 여부를 나타냅니다.

  1. 개체 탭에서 개체 유형(이 예제에서개체 > 주소)을 선택합니다.
  2. 개체를 추가한 디바이스 그룹을 선택합니다.

     개체 탭에는 선택한 디바이스 그룹에 있거나 상위 디바이스 그룹 또는 공유 위치에서 상속된 개체만 표시됩니다.
  3. 디바이스 그룹 개체가 나타나는지 확인합니다. 위치 열의 디바이스 그룹 이름은 디바이스 그룹 드롭다운의 선택과 일치합니다.

상속된 개체 값으로 되돌리기

디바이스 그룹 객체가 상위 디바이스 그룹에서 상속하는 값을 재정의한 후에는 언제든지 객체를 상위 값으로 되돌릴 수 있습니다. 개체 탭에서 재정의된 개체는 이름 열에 노란색-중복-녹색 아이콘()이 있습니다.

특정 객체를 되돌리는 대신 모든 재정의된 객체에 조상 값을 푸시하려면 상속된 개체의 우선 순위 관리을(를) 참조하십시오.

값을 재정의하는 단계는 5단계를 참조하십시오.

객체 상속 및 재정의에 대한 자세한 내용은 디바이스 그룹 개체을(를) 참조하십시오.

STEP 1 | 개체 탭에서 개체 유형(예: 개체 > 주소)을 선택한 다음 개체의 재정의 인스턴스가 있는 디바이스 그룹을 선택합니다.

STEP 2 | 개체를 선택한 다음 되돌리기를 클릭한 다음 예를 클릭합니다. 이름 열에 개체에 대한 녹색 아이콘이 표시되어 개체가 이제 상위 디바이스 그룹의 모든 값을 상속함을 나타냅니다.

STEP 3 | 커밋 > 커밋 및 푸시를 선택한 다음 Panorama 구성 및 객체를 되돌린 디바이스 그룹에 대한 변경 사항을 커밋 및 푸시합니다.

미사용 공유 객체 관리

구성 변경 사항 디바이스 그룹을(를) 푸시하면 기본적으로 Panorama는 공유 또는 장치 그룹 정책 규칙이 개체를 참조하는지 여부에 관계없이 모든 공유 개체를 방화벽으로 푸시합니다. 그러나 디바이스 그룹에서 규칙이 참조하는 공유 객체만 푸시하도록 Panorama를 구성할 수 있습니다. 사용하지 않는 주소 및 서비스 개체를 디바이스와 공유 옵션을 사용하면 Panorama가 관리되는 방화벽으로 푸시하는 개체를 제한할 수 있습니다.

사용하지 않는 주소 및 서비스 개체를 디바이스와 공유가 비활성화된 경우 *Panorama*는 방화벽의 하위 집합에 정책 규칙 푸시을(를) 수행할 때 대상을 무시합니다. 즉, 규칙에서 참조하는 모든 개체가 디바이스 그룹의 모든 방화벽으로 푸시됩니다.

관리되는 방화벽 집합에 푸시되는 개체 수를 제한하려면 정책 규칙을 하위 디바이스 그룹에 추가하고 필요에 따라 공유 개체를 참조하십시오. 하위 디바이스 그룹 생성에 대한 자세한 내용은 디바이스 그룹 계층 생성을(를) 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

PA-220과 같은 로우엔드 모델에서는 관련 공유 개체만 관리되는 방화벽으로 푸시하는 것을 고려하십시오. 보급형 모델에 저장할 수 있는 개체의 수가 중급 이상 모델에 비해 현저히 적기 때문입니다. 또한 사용하지 않는 주소 및 서비스 개체가 많은 경우 디바이스와 사용하지 않는 주소 및 서비스 개체 공유를 지우면 각 방화벽에 푸시되는 구성이 더 작아지므로 방화벽에서 커밋 시간이 크게 줄어듭니다. 그러나 Panorama는 정책 규칙이 특정 개체를 참조하는지의 여부를 동적으로 확인해야 하므로 이 옵션을 비활성화하면 Panorama에서 커밋 시간이 늘어날 수 있습니다.

STEP 1 | **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.

STEP 2 | 규칙이 참조하는 공유 개체만 푸시하려면 디바이스와 사용하지 않는 주소 및 서비스 개체 공유 옵션을 지우거나 모든 공유 개체 푸시를 다시 활성화하려면 옵션을 선택합니다.

이 옵션을 선택 취소하면 *Panorama*가 모든 정책에서 개체에 대한 참조를 확인해야 하며 구성에 따라 커밋 시간이 늘어날 수 있습니다.

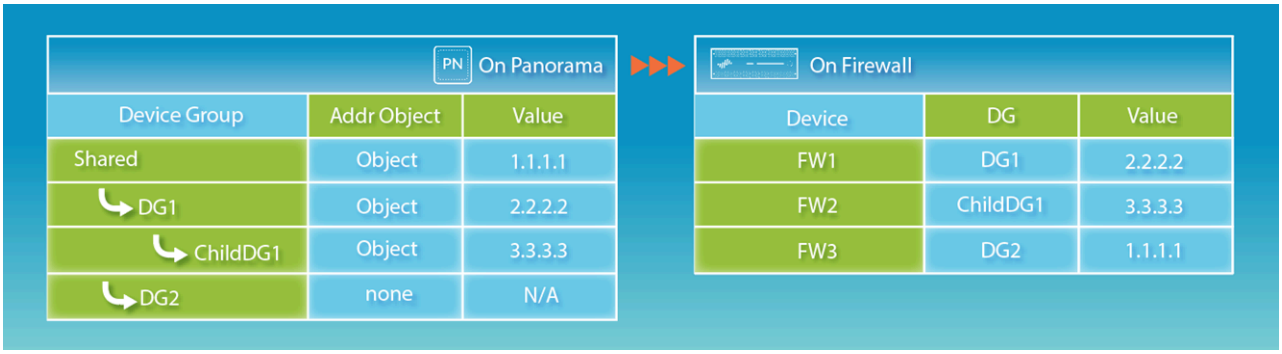
(모범 사례) 향후 모든 커밋에 대해 이 옵션을 선택 취소하려면 커밋 시간을 줄일 수 있도록 공유 구성 개체 수를 제한하십시오.

STEP 3 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 4 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

상속된 개체의 우선 순위 관리

기본적으로 디바이스 그룹 계층의 다른 수준에 있는 디바이스 그룹에 이름은 같지만 값이 다른 개체가 있는 경우(예: 재정의로 인해) 하위 디바이스 그룹의 정책 규칙은 개체 값을 사용하는 대신 상위 디바이스 그룹에서 상속된 해당 하위 항목의 개체 값을 사용합니다. 선택적으로 이 우선 순위를 반대로 하여 개체를 포함하는 가장 높은 상위 항목의 값을 모든 하위 디바이스 그룹으로 푸시할 수 있습니다. 이 옵션을 활성화하면 다음에 구성 변경 사항을 디바이스 그룹에 푸시할 때 상속된 개체의 값이 하위 디바이스 그룹에서 재정의된 개체의 값을 대체합니다. 아래 그림은 디바이스 그룹에서 상속된 개체의 우선 순위를 보여줍니다.



방화벽에 *Panorama*가 푸시하는 공유 또는 디바이스 그룹 개체와 이름이 같은 개체가 로컬로 정의되어 있으면 커밋 실패가 발생합니다.

오버라이드된 모든 객체에 상위 값을 푸시하는 대신 오버라이드된 특정 객체를 상위 값으로 되돌리려면 상속된 개체 값으로 되돌리기을(를) 참조하십시오.

STEP 1 | **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 기본 우선 순위를 반대로 하려면 상위 항목에 정의된 개체가 더 높은 우선 순위를 가짐을 선택합니다. 그런 다음 대화 상자는 재정의된 개체 찾기 링크를 표시합니다. 이 링크는 이 변경 사항을 커밋한 후 얼마나 많은 재정의된(그림자) 개체에 상위 값이 있는지 확인하는 옵션을 제공합니다. 수량 메시지 위로 마우스를 가져가면 개체 이름이 표시됩니다.

기본 우선 순위로 되돌리려면 상위 항목에 정의된 클리어 개체가 더 높은 우선 순위를 갖습니다.

재정의된 개체 찾기는 디바이스 그룹의 다른 개체와 이름을 공유하는 공유 디바이스 그룹 개체만 감지합니다.

STEP 3 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 4 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

STEP 5 | (선택 사항) 상위 항목에 정의된 개체가 더 높은 우선 순위를 가짐을 선택한 경우 Panorama는 구성 변경 사항을 디바이스 그룹에 푸시할 때까지 상위 개체를 푸시하지 않습니다. 커밋 > 디바이스에 푸시를 선택한 다음 변경 사항을 푸시합니다.

정책 규칙 또는 다른 디바이스 그룹으로 이동 또는 복제

Panorama에서 디바이스 그룹에서 이동하거나 복제할 정책 규칙 또는 개체가 대상 디바이스 그룹(대상)에서 사용할 수 없는 개체에 대한 참조가 있는 경우 참조된 개체 및 참조 규칙 또는 객체를 동일한 작업에서 이동하거나 복제해야 합니다. 디바이스 그룹 계층구조에서, 참조된 개체는 상속을 통해 사용할 수 있습니다. 예를 들어 공유 개체는 모든 디바이스 그룹에서 사용할 수 있습니다. 전역 찾기를 수행하여 참조를 확인할 수 있습니다. 재정의된 개체를 이동하거나 복제하는 경우 대상의 상위 디바이스 그룹에서 해당 개체에 대한 재정의가 활성화되어 있는지 확인합니다(공유 또는 디바이스 그룹정책에서 사용할 개체 생성 참조).

여러 정책 규칙을 복제할 때 규칙을 선택하는 순서는 디바이스 그룹에 복사되는 순서를 결정합니다. 예를 들어, 규칙 *1-4*가 있고 선택 순서가 *2-1-4-3*인 경우 이러한 규칙이 복사될 디바이스 그룹은 선택한 것과 동일한 순서로 규칙을 표시합니다. 그러나 성공적으로 복사되면 규칙을 적절하게 재구성할 수 있습니다.

STEP 1 | Panorama에 로그인하고 규칙 자료(예: 정책 > 보안 > 사전 규칙) 또는 개체 유형(예: 개체 > 주소)을 선택합니다.

STEP 2 | 디바이스 그룹을 선택한 다음 하나 이상의 규칙 또는 개체를 선택합니다.

STEP 3 | 다음 단계 중 하나를 수행합니다.

- (규칙만) 다른 > 디바이스 그룹으로 이동
- (객체만) 이동
- (규칙 또는 객체) 복제

STEP 4 | 대상 드롭다운에서 새 디바이스 그룹 또는 공유를 선택합니다. 기본값은 이전에 선택된 디바이스 그룹입니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | (규칙만) 규칙 순서를 선택합니다.

- 맨 위로 이동(기본값) - 규칙이 다른 모든 규칙보다 먼저 표시됩니다.
- 맨 아래로 이동 - 규칙이 다른 모든 규칙 다음에 옵니다.
- 사전 규칙 - 인접한 드롭다운에서 선택한 규칙 다음에 오는 규칙을 선택합니다.
- 사후 규칙 - 인접한 드롭다운에서 선택한 규칙 앞에 오는 규칙을 선택합니다.

STEP 6 | 유효성 검사 확인란에서 처음 감지된 오류에 대한 오류는 기본적으로 선택되므로 Panorama가 찾은 첫 번째 오류가 표시되고 더 많은 오류 확인을 중지합니다. 예를 들어 대상 디바이스 그룹에 이동하는 규칙에서 참조되는 개체가 없는 경우 오류가 발생합니다. 여러 항목을 한 번에 이동하거나 복제하면 이 체크박스을 선택하면 문제 해결이 간소화될 수 있습니다. 체크박스을 지우면 Panorama가 표시하기 전에 모든 오류를 발견합니다. 이 설정에 관계없이 Panorama는 선택한 모든 항목에 대한 모든 오류를 해결할 때까지 아무것도 이동하거나 복제하지 않습니다.

STEP 7 | 확인을 클릭하여 오류 유효성 검사를 시작합니다. Panorama가 오류를 발견하면 수정하고 이동 또는 복제 작업을 다시 시도합니다. Panorama에 오류가 없는 경우 작업을 수행합니다.

STEP 8 | 커밋 > 커밋 및 푸시를 선택한 다음 푸시 범위에서 선택 편집하고, 디바이스 그룹을 선택한 다음, 원본 및 대상 디바이스 그룹을 선택하고, 확인을 클릭한 다음, Panorama 구성 및 디바이스 그룹에 변경 내용을 커밋하고 푸시합니다.

원본 또는 대상 디바이스 그룹에 디바이스가 없는 경우 모든 변경 사항을 푸시해야 합니다. 선택적 푸시는 디바이스가 없는 디바이스 그룹에 대해 지원되지 않습니다.

방화벽의 하위 집합에 정책 규칙 푸시

정책 대상을 사용하면 정책 규칙을 푸시할 디바이스 그룹의 방화벽을 지정할 수 있습니다. 하나 이상의 방화벽 또는 가상 시스템을 제외하거나 디바이스 그룹의 특정 방화벽 또는 가상 시스템에만 규칙을 적용할 수 있습니다.

규칙 베이스가 발전하고 새 규칙이나 수정된 규칙을 방화벽에 푸시하면 규칙이 생성되거나 수정될 때 보관되지 않는 한 변경 사항 및 감사 정보가 시간이 지남에 따라 손실됩니다. 감사 설명 아카이브를 사용하여 선택한 규칙의 감사 설명 및 구성 로그 기록을 보고 두 정책 규칙 버전을 비교하여 규칙이 어떻게 변경되었는지 확인합니다. Panorama에서 푸시된 규칙에 대한 감사 설명 기록은 Panorama 관리 서버에서만 볼 수 있습니다. 그러나 관리 방화벽에서 Panorama로 포워딩된 구성 로그에서 감사 설명을 볼 수 있습니다. 그러나 방화벽에서 로컬로 생성 또는 수정된 규칙에 대해서는 감사 주석 아카이브를 볼 수 없습니다. 규칙이 생성되거나 수정될 때 감사 주석이 캡처되도록 하려면 정책 규칙, 설명, 태그 및 감사 주석을 적용합니다.

규칙을 대상으로 지정하는 기능을 사용하면 Panorama에서 정책을 중앙 집중식으로 유지할 수 있습니다. 대상 규칙을 사용하면 Panorama에서 규칙(공유 또는 디바이스 그룹 사전 또는 사후 규칙으로)을 정의하고 규칙을 관리할 때 가시성과 효율성을 개선할 수 있습니다(디바이스 그룹 정책 참조). 감사 주석 아카이브는 시간 경과에 따라 정책 규칙이 변경되는 방식과 이유를 추적하여 규칙 수명 주기 동안 규칙 진화를 감사할 수 있도록 하여 가시성을 추가합니다.

©2024 Palo Alto Networks, Inc.

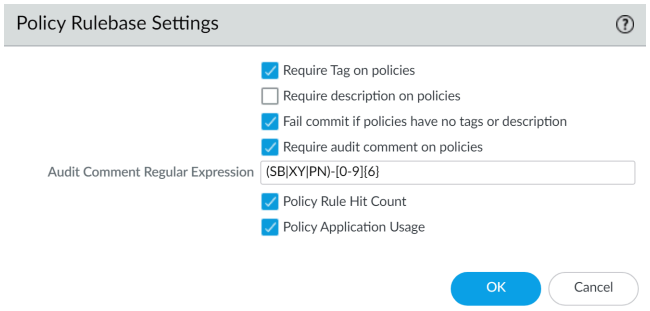
STEP 1 | (모범 사례) 정책 규칙에 대한 감사 의견을 시행합니다.

이 단계는 선택 사항이지만 규칙을 만들거나 수정하는 이유를 캡처할 수 있도록 정책 규칙에 대한 감사 설명을 적용하는 것이 가장 좋습니다. 이는 또한 감사 목적으로 정확한 규칙 기록을 유지하는 데 도움이 됩니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 정책 규칙 베이스 설정을 편집합니다.
2. 정책에 대한 감사 설명 필요 옵션을 활성화합니다.
3. 감사 주석 정규식을 구성하여 감사 주석 형식을 지정합니다.

   규칙을 만들거나 수정할 때 문자 및 숫자 식을 지정하여 비즈니스 및 감사 요구 사항에 따라 특정 형식을 준수하도록 감사 주석을 요구합니다. 예를 들어, 이 설정을 사용하여 발권 번호 형식과 일치하도록 정규 표현식을 지정할 수 있습니다.

   - **[0-9]{<Number of digits>}** - 감사 주석에 0에서 9 사이의 최소 자릿수를 포함해야 합니다. 예를 들어, **[0-9]{6}**에는 0에서 9 사이의 숫자가 포함된 최소 6자리 숫자 표현식이 필요합니다. 필요에 따라 최소 자릿수를 구성합니다.
   - **<## ###>** - 감사 주석에 문자 표현식이 포함되어야 합니다. 예를 들어 **## ##** - 관리자는 이 문자 표현으로 감사 설명을 시작해야 합니다.
   - **<## #>-[0-9]{<Number of digits>}** - 감사 주석에 최소 자릿수가 0에서 9 사이인 설정된 문자 접두어가 포함되어야 합니다. 예를 들어, **SB-[0-9]{6}**는 **SB-012345**와 같이 숫자 0에서 9까지의 최소 6자리 숫자 표현식이 뒤에 오는 **SB-**로 시작하는 감사 주석 형식을 요구합니다.
   - **(<## #>)|(<## #>)|(<Letter ## #>)|-[0-9]{<Number of digits>}** - 감사 주석에 0에서 9 사이의 최소 자릿수를 가진 문자 표현식으로 구성된 집합 중 하나를 사용하여 접두사를 포함해야 합니다. 예를 들어, **(SB|XY|PN)-[0-9]{6}**는 감사 설명 형식이 **SB-**, **XY-** 또는 **PN-**으로 시작하고 **SB-012345**, **XY-654321** 또는 **PN-012543**과 같이 그 뒤에 숫자 0에서 9까지의 최소 6자리 숫자 표현식이 필요합니다.
4. 확인을 클릭하여 새 정책 규칙 베이스 설정을 적용합니다.



5. 커밋 및 **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | 규칙을 생성합니다.

이 예에서는 내부 네트워크의 사용자가 DMZ의 서버에 액세스할 수 있도록 허용하는 사전 규칙을 보안 규칙 베이스에 정의합니다.

1. 정책 탭에서 규칙을 정의할 디바이스 그룹을 선택합니다.
2. 규칙 베이스를 선택합니다. 이 예에서는 정책 > 보안 > 사전 규칙 및 규칙 추가를 선택합니다.
3. 일반 탭에서 설명 규칙 이름을 입력하고 감사 설명을 입력합니다.
4. 원본 탭에서 원본 영역을 신뢰로 설정합니다.
5. 대상 탭에서 대상 영역을 **DMZ**로 설정합니다.
6. 서비스/**URL** 카테고리 탭에서 서비스를 **application-default**로 설정합니다.
7. 작업 탭에서 작업을 허용으로 설정합니다.
8. 다른 모든 옵션은 기본값으로 설정된 상태로 둡니다.

STEP 3 | 방화벽의 하위 집합을 포함하거나 제외하도록 규칙을 대상으로 지정합니다.

선택한 방화벽 집합에 규칙을 적용하려면 다음을 수행합니다.

1. 정책 규칙 대화 상자에서 대상 탭을 선택합니다.
2. 규칙을 적용할 방화벽을 선택합니다.

   대상 태그 또는 대상 디바이스 중 하나만 선택했는지 확인합니다. 대상 태그와 대상 디바이스를 모두 선택하면 구성 푸시가 실패할 수 있습니다.

   대상으로 방화벽을 선택하지 않으면 디바이스 그룹의 모든(선택되지 않은) 방화벽에 규칙이 추가됩니다.

   기본적으로 디바이스 그룹의 가상 시스템에 대한 체크박스은 비활성화되어 있지만 규칙을 적용할 가상 시스템을 하나 이상 선택하지 않는 한 모든 가상 시스템은 커밋 시 규칙을 상속합니다.
3. (선택 사항) 규칙 상속에서 방화벽 하위 집합을 제외하려면 지정된 디바이스를 제외한 모든 디바이스에 설치하고 제외할 방화벽을 선택합니다.

   지정된 디바이스를 제외한 모든 디바이스에 설치하고 방화벽을 선택하지 않으면 디바이스 그룹의 방화벽에 규칙이 추가되지 않습니다.
4. 확인을 클릭하여 규칙을 추가합니다.

STEP 4 | 구성 변경 사항을 커밋하고 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 디바이스 그룹을 선택한 다음 규칙을 추가한 디바이스 그룹을 선택한 다음 확인을 클릭합니다.
3. (선택 사항) Panorama의 구성 변경과 별도로 로컬 방화벽 구성 변경을 관리하는 경우디바이스 후보 구성과 병합을 비활성화합니다.

   이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 Panorama의 구성 푸시와 병합합니다. 로컬 방화벽 구성은 Panorama에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 로컬 방화벽 구성이 병합되고 커밋됩니다.
4. Panorama 구성 및 디바이스 그룹에 대한 변경 사항을 커밋하고 푸시합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 정책 규칙 트래픽 일치 문제 해결 규칙이 의도한 대로 트래픽을 허용하고 거부하는지 확인합니다.

Multi-VSYS 방화벽으로 디바이스 그룹 푸시

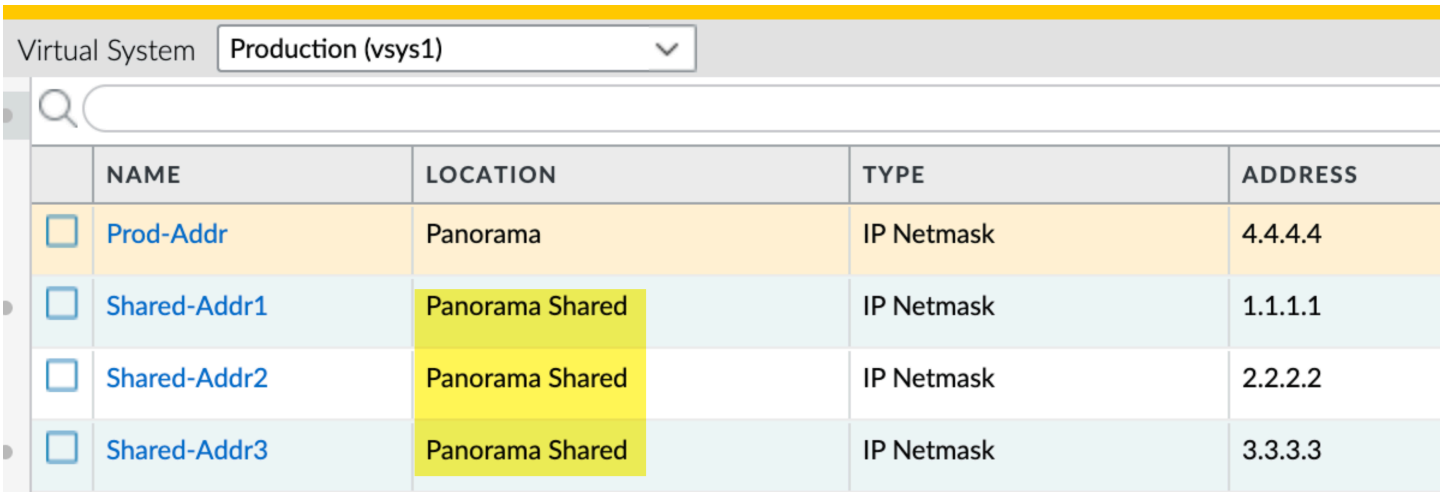
Panorama™ 관리 서버에서 Multi-VSYS 방화벽으로 디바이스 그룹을 수동으로 푸시하거나 예약된 구성 푸시에서 푸시된 디바이스 그룹 구성 변경 사항은 자동으로 단일 작업으로 번들링됩니다. Panorama에서 관리 방화벽으로 푸시가 실행되면 Panorama는 디바이스 그룹 푸시와 연결된 관리 방화벽을 검사합니다. Panorama는 동일한 Multi-VSYS 방화벽에 속한 여러 vsys가 디바이스 그룹 푸시와 연결되어 있음을 감지하면 각 vsys에 대한 커밋 작업을 관리되는 방화벽의 단일 커밋 작업으로 묶어 전체 커밋 작업 완료 시간을 줄입니다.

번들 커밋 작업 중 하나가 실패하면 전체 푸시가 실패하고 Panorama에서 전체 디바이스 그룹 구성 변경 사항을 다시 푸시해야 합니다. 또한 Panorama의 푸시에 다중 가상 시스템 방화벽이 여러 개 포함되어 있고 한 번의 푸시가 실패하면 Panorama의 푸시에 포함된 모든 방화벽에 대한 전체 푸시가 실패합니다. 디바이스 그룹 푸시를 방화벽에서 로컬로 모니터링하면 여러 개별 작업이 아닌 단일 작업이 표시됩니다. 경고가 실패하면 영향을 받는 vsys를 나타내는 오류에 대한 설명이 표시됩니다.

이 기능은 기본적으로 PAN-OS 10.2 이상의 버전을 실행하는 Panorama에서 관리하는 Multi-VSYS 방화벽에서 지원됩니다. Palo Alto Networks는 Multi-VSYS 관리형 방화벽의 모든 vsys를 Panorama에서 관리하도록 권장합니다. PAN-OS 10.2로 업그레이드한 후에는 Panorama에서 관리형 방화벽으로 완전히 커밋하고 푸시해야 아래에 설명한 대로 공유 개체 푸시를 Multi-VSYS 방화벽으로 최적화하는 관리자 수준 푸시를 수행할 수 있습니다. 업그레이드 후 완전히 커밋하고 푸시하지 않으면 중복 개체로 인해 Multi-VSYS 방화벽에 대한 모든 후속 푸시가 실패하고 모든 공유 구성 개체가 최적화된 `Panorama ##` 위치가 아닌 `Panorama` 위치에 저장됩니다.

다중 VSYS 방화벽에 푸시된 공유 개체

다중 가상 시스템 방화벽에 대한 구성 조정의 운영 부담을 줄이기 위해 다중 가상 시스템 방화벽에 푸시된 공유 구성 개체는 관리되는 다중 가상 시스템 방화벽의 Panorama 공유 위치로 푸시됩니다. Panorama 공유 위치는 방화벽의 모든 가상 시스템에서 사용할 수 있습니다. 즉, 공유 개체가 각 가상 시스템에 복제되지 않습니다.



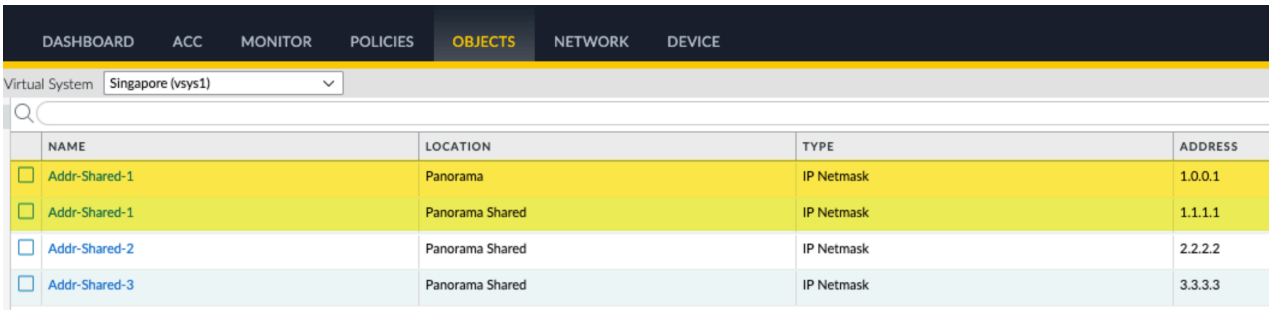
 ©2024 Palo Alto Networks, Inc.

다음 구성은 공유 *Panorama* 위치에 추가할 수 없으며 다중 가상 시스템 방화벽의 각 가상 시스템의 *Panorama* 위치에 복제됩니다.

- 사전 및 사후 규칙
- 외부 동적 목록*(EDL)*
- 보안 프로파일 그룹
- *HIP* 개체 및 프로필
- 맞춤 *URL* 개체
- 암호 해독 프로필
- *SD-WAN* 링크 관리 프로필

Panorama Shared 개체가 디바이스 그룹에서 재정의되면 이름은 같지만 재정의된 값을 가진 새 개체가 해당 디바이스 그룹의 Panorama 위치에 만들어지고 다중 가상 시스템 방화벽의 모든 가상 시스템에 푸시됩니다. Panorama 및 Panorama Shared 위치 모두에 동일한 이름의 구성 개체가 있는 경우 방화벽의 해당 vsys에 고유하므로 Panorama 위치의 개체에 구성이 우선 적용됩니다.

예를 들어 아래의 vsys는 Panorama 및 Panorama 위치 모두에 있는 `Addr-Shared-1` 주소 개체를 보여줍니다. `Addr-Shared-1` 개체가 정책 규칙에서 사용되는 경우 `1.0.0.1` IP 주소가 사용됩니다.



규칙 계층 구조 관리

정책 규칙순서는 네트워크 보안에 매우 중요합니다. 모든 정책 계층(공유, 디바이스 그룹 또는 로컬로 정의된 규칙) 및 규칙 기반(예: 공유 보안 사전 규칙)에서 방화벽은 정책 탭 페이지에 나타나는 순서대로 위에서 아래로 규칙을 평가합니다. 방화벽은 정의된 기준을 충족하고 후속 규칙을 무시하는 첫 번째 규칙과 패킷을 일치시킵니다. 따라서 가장 구체적인 일치를 적용하려면 보다 일반적인 규칙 위에 더 구체적인 규칙을 위치시킵니다.

디바이스 그룹 계층에서 방화벽이 계층 및 유형(사전 규칙, 사후 규칙 및 기본 규칙)별로 규칙을 평가하는 순서를 이해하려면 디바이스 그룹 정책을 참조하십시오.

STEP 1 | 각 규칙베이스에 대한 규칙 계층 구조를 봅니다.

1. 정책 탭을 선택한 다음 미리보기 규칙을 클릭합니다.

©2024 Palo Alto Networks, Inc.

2. 규칙베이스(예: 보안 또는 **QoS**)로 미리 보기를 필터링합니다.
3. 미리 보기를 필터링하여 특정 디바이스 그룹의 규칙과 공유 위치 및 상위 디바이스 그룹에서 상속하는 규칙을 표시합니다. 방화벽이 할당된 디바이스 그룹을 선택해야 합니다.
4. 디바이스에서 미리 보기를 필터링하여 로컬로 정의된 규칙을 표시합니다.
5. 녹색 화살표 아이콘을 클릭하여 미리 보기에 필터 선택을 적용합니다(디바이스 그룹 정책 참조).
6. 규칙 미리 보기를 완료하면 결합된 규칙 미리 보기 대화 상자를 닫습니다.

STEP 2 | 필요한 경우 규칙을 삭제하거나 비활성화합니다.



방화벽이 현재 사용하지 않는 규칙을 확인하려면 *Panorama*의 컨텍스트 드롭다운에서 해당 방화벽을 선택한 다음 규칙 기반(예: 정책 > 보안)을 선택한 다음 사용하지 않는 규칙 표시란을 선택합니다. 점선 주황색 배경은 방화벽이 사용하지 않는 규칙을 나타냅니다.

1. 삭제 또는 비활성화할 규칙을 포함하는 규칙 기반(예: 정책 > 보안 > 사전 규칙)을 선택합니다.
2. 규칙이 포함된 디바이스 그룹을 선택합니다.
3. 규칙을 선택한 다음 원하는 대로 삭제 또는 비활성화를 클릭합니다. 비활성화된 규칙은 기울임꼴로 표시됩니다.

STEP 3 | 필요한 경우 규칙 베이스 내에서 재배치 규칙입니다.



방화벽에서 로컬 규칙을 재배치하려면 이 단계를 수행하기 전에 컨텍스트 드롭다운에서 해당 방화벽을 선택하여 웹 인터페이스에 액세스합니다.

1. 이동할 규칙을 포함하는 규칙 기반(예: 정책 > 보안 > 사전 규칙)을 선택합니다.
2. 규칙이 포함된 디바이스 그룹을 선택합니다.
3. 규칙을 선택한 다음 이동을 선택한 다음 다음을 선택합니다.
   - 위쪽이동— 디바이스 그룹의 다른 모든 규칙 위에 해당 규칙을 이동시킵니다(공유 또는 상위 디바이스 그룹에서 상속된 규칙 위의 경우는 제외).
   - 위로이동—이전 규칙 위에 해당 규칙을 이동시킵니다(공유 또는 조상 디바이스 그룹에서 상속된 규칙 위는 아님).
   - 아래로이동—규칙을 따르는 규칙 아래로 이동합니다.
   - 아래쪽이동—규칙을 다른 모든 규칙 아래로 이동합니다.
   - 다른 디바이스 그룹으로이동—정책 규칙 또는 개체를 다른 디바이스 그룹으로 이동 또는 복제를 참조하십시오.

STEP 4 | 규칙을 수정한 경우 변경 내용을 커밋하고 푸시합니다.

1. 푸시 범위에서 커밋 > 머킷 및 푸시 및 선택 편집을 선택합니다.
2. 디바이스 그룹을 선택한 다음 변경하거나 삭제한 규칙이 포함된 디바이스 그룹을 선택하고 확인을 클릭합니다.
3. Panorama 구성 및 디바이스 그룹에 대한 변경 사항을 커밋하고 푸시합니다.

©2024 Palo Alto Networks, Inc.

템플릿 및 템플릿 스택(template stack) 관리

템플릿 및 템플릿 스택(template stack)을 사용하여 네트워크에서 방화벽이 작동할 수 있도록 하는 공통 기본 구성을 정의합니다. 어떤 방화벽을 어떤 템플릿에 추가할지를 결정할 때 고려해야 하는 문제에 대한 개요는 템플릿 및 템플릿 스택(template stack)을 참조하십시오.

템플릿을 삭제하려면 먼저 방화벽에서 템플릿 설정을 로컬로 비활성화/제거를 해야 합니다. 운용 관리자 역할이 있는 관리자만 템플릿을 비활성화할 수 있습니다.

- 템플릿 기능 및 예외
- 템플릿 추가
- 템플릿 스택(template stack) 구성
- 템플릿 또는 템플릿 스택(template stack) 변수 구성
- 기존 템플릿 스택(template stack) 변수 가져오기 및 덮어쓰기
- 템플릿 설정 재정의
- 템플릿 설정 비활성화/제거

템플릿 기능 및 예외

템플릿 및 템플릿 스택(template stack)을 사용하여 다양한 설정을 정의할 수 있지만 다음 작업은 각 관리 방화벽에서 로컬로만 수행할 수 있습니다.

- 디바이스 차단 목록을 구성합니다.
- 로그를 지웁니다.
- 일반 모드, Multi-VSYS 모드 또는 FIPS-CC 모드와 같은 작동 모드를 활성화합니다.
- HA 쌍에서 방화벽의 IP 주소를 구성합니다.
- 마스터 키 및 진단을 구성합니다.
- 구성 파일을 비교합니다(구성 감사).

  방화벽에 대한 라이선스 및 업데이트(소프트웨어 또는 콘텐츠)를 관리하려면 ***Panorama*** > ***Device Management*** 탭 옵션을 사용하십시오. 템플릿을 사용하지 마십시오.
- Multi-VSYS 방화벽에서 vsys 이름 바꾸기.

템플릿 추가

Panorama™가 방화벽에 대한 네트워크 설정 및 디바이스 구성 요소를 정의하는 데 필요한 디바이스 및 네트워크 탭을 표시하기 전에 하나 이상의 템플릿을 추가해야 합니다. Panorama는 최대 1,024개의 템플릿을 지원합니다. 모든 관리 방화벽은 템플릿 스택(template stack)에 속해야 합니다. 템플릿에는 관리 디바이스 구성이 포함되어 있지만 템플릿 스택(template stack)을 사용하면 템플릿 구성을 관리하고 템플릿 스택(template stack)에 할당된 모든 관리 방화벽에 푸시할 수 있습니다.

©2024 Palo Alto Networks, Inc.

템플릿 간에 많은 구성이 중복되지 않도록 템플릿 스택*(template stack)*에 템플릿을 결합합니다*(*템플릿 및 템플릿 스택(template stack) 및 템플릿 스택(template stack) 구성 참조*)*.

STEP 1 | 템플릿을 추가합니다.

1. **Panorama** > 템플릿을 선택합니다.
2. 추가를 클릭하고 템플릿을 식별할 고유한 이름을 입력합니다.
3. (선택 사항) 템플릿에 대한 설명을 입력합니다.
4. 확인을 클릭하여 템플릿을 저장합니다.
5. 템플릿에 가상 시스템이 없는 방화벽에 Panorama를 푸시할 구성(예: 인터페이스)이 있는 가상 시스템(vsys)이 있는 경우 생성한 템플릿을 선택하고 기본 **VSYS** 드롭다운에서 vsys를 선택한 다음 확인을 클릭합니다.
6. 커밋 > 커밋 및 푸시를 선택한 다음 Panorama 구성 및 템플릿에 대한 변경 사항을 커밋 및 푸시합니다.

STEP 2 | 템플릿을 사용할 수 있는지 확인합니다.

첫 번째 템플릿을 추가하면 Panorama에 디바이스 및 네트워크 탭이 표시됩니다. 이러한 탭에는 템플릿 드롭다운이 표시됩니다. 드롭다운에 방금 추가한 템플릿이 표시되는지 확인합니다.

STEP 3 | 템플릿 스택을 구성하고 템플릿 스택에 템플릿을 추가합니다.

 ©2024 Palo Alto Networks, Inc.

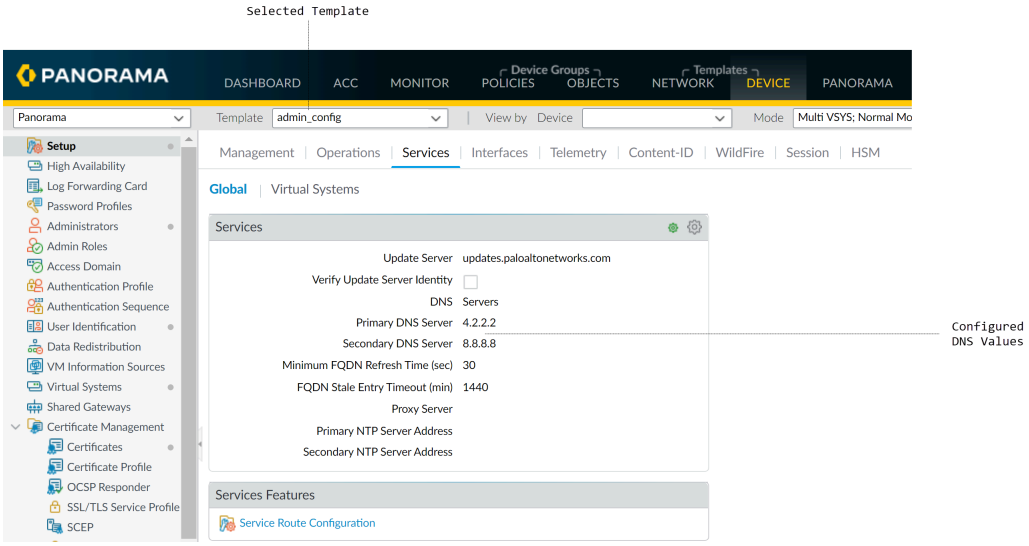
STEP 4 | 템플릿을 사용하여 구성 변경 사항을 방화벽에 푸시합니다.

vsys 이름 바꾸기는 *Panorama*가 아닌 로컬 방화벽에서만 허용되며 결과적으로 완전히 새로운 *vsys*가 생성되거나 새 *vsys* 이름이 방화벽의 잘못된 *vsys*에 매핑됩니다.

예를 들어 템플릿에서 방화벽에 대한 기본 DNS(Domain Name System) 서버를 정의합니다.

템플릿 또는 템플릿 스택(template stack) 변수를 구성하여 디바이스별 값을 관리되는 디바이스로 푸시할 수도 있습니다.

1. 디바이스 탭의 드롭다운에서 템플릿을 선택합니다.
2. 디바이스 > 설정 > 서비스 > 전역을 선택하고 서비스 섹션을 편집합니다.
3. 기본 **DNS** 서버의 IP 주소를 입력합니다.

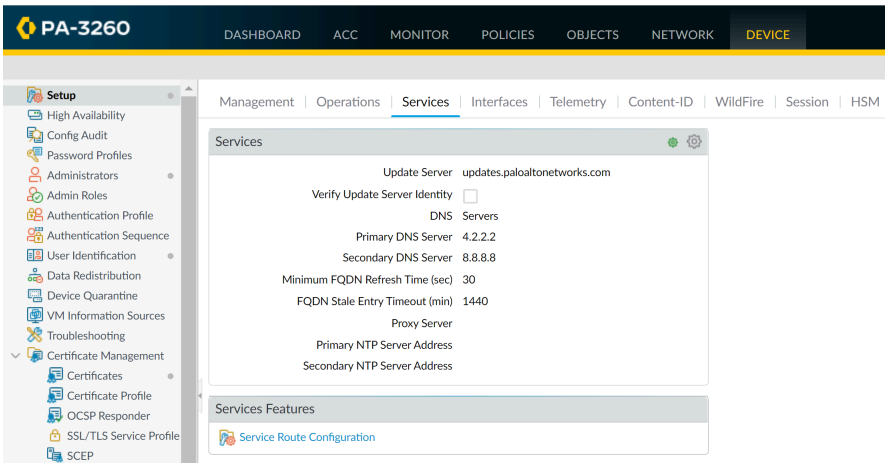


4. 커밋 > 커밋 및 푸시를 선택한 다음 Panorama 구성 및 템플릿에 대한 변경 사항을 커밋 및 푸시합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama에서 푸시한 템플릿 설정으로 방화벽이 구성되어 있는지 확인합니다.

1. 컨텍스트 드롭다운에서 템플릿 설정을 푸시한 방화벽 중 하나를 선택합니다.
2. 디바이스 > 설정 > 서비스 > 전역을 선택합니다. 템플릿에서 푸시한 IP 주소가 나타납니다. 서비스 섹션 헤더에는 섹션의 설정에 템플릿에서 푸시된 값이 있음을 나타내는 템플릿 아이콘( )이 표시됩니다.



STEP 6 | 방화벽이 네트워크 리소스에 액세스할 수 있는지 확인하기 위해 네트워크 리소스에 대한 연결 문제 해결을(를) 수행합니다.

템플릿 스택(template stack) 구성

템플릿 스택(template stack)을 구성할 수 있으며 여러 템플릿을 결합하여 관리되는 방화벽에 전체 구성을 푸시할 수 있습니다. 템플릿은 여러 스택에서 재사용할 수 있는 방화벽 구성의 모듈식 부분이지만 스택에 할당된 모든 방화벽에 적용해야 하는 나머지 구성을 채우도록 템플릿 스택(template stack)을 구성할 수도 있습니다. Panorama는 최대 1,024개의 템플릿 스택(template stack)을 지원하며 각 스택에는 최대 8개의 템플릿이 할당될 수 있습니다. 템플릿 스택에 속한 템플릿에서 템플릿 스택에 구성된 개체를 참조할 수 있습니다. 템플릿 스택(template stack)은 추가한 템플릿에서 구성 객체를 상속하며 템플릿 스택(template stack)에서 템플릿을 주문하는 방법을 기반으로 합니다. 템플릿 스택(template stack)의 템플릿 설정을 재정의하여 템플릿 스택(template stack) 구성 객체를 생성할 수도 있습니다. 자세한 내용 및 계획은 템플릿 및 템플릿 스택을 참조하십시오.

인터페이스, *VLAN*, 가상 와이어, *IPSec* 터널, *DNS* 프록시 및 가상 시스템을 구성하는 템플릿을 추가합니다. 이러한 개체는 템플릿 스택*(template stack)*이 아니라 템플릿에서 구성 및 푸시해야 합니다. 템플릿에서 푸시되면 템플릿 스택에서 가상 시스템을 제외한 이러한 개체를 재정의할 수 있습니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 템플릿과 스택의 순서를 계획합니다.

템플릿 스택(template stack)에 할당하려는 템플릿을 추가합니다.

스택 내 템플릿의 우선 순위를 계획할 때(겹치는 설정의 경우) 잘못된 구성을 방지하기 위해 순서를 확인해야 합니다. 예를 들어, *ethernet1/1* 인터페이스가 *Template_A*의 유형 *3*이지만 *Template_B*의 *VLAN*이 있는 유형 *2*인 스택을 고려하십시오. *Template_A*의 우선 순위가 더 높으면 *Panorama*는 *ethernet1/1*을 레이어 *3* 유형으로 푸시하지만 *VLAN*에 할당됩니다.

또한 템플릿 구성은 두 템플릿이 동일한 스택에 있더라도 다른 템플릿의 구성을 참조할 수 없습니다. 예를 들어, Template_A의 영역 구성은 Template_B의 영역 보호 프로파일을 참조할 수 없습니다.

STEP 2 | 템플릿 스택(template stack)을 생성합니다.

1. **Panorama** > 템플릿을 선택한 다음 스택 추가를 선택합니다.

   *Panorama*는 스택 추가만 지원하여 새 템플릿 스택을 생성합니다. 기존 템플릿 스택은 복제할 수 없습니다.

2. 스택을 식별할 고유 이름을 입력합니다.
3. (선택 사항) 템플릿 스택에 대한설명을 추가합니다.
4. (선택 사항) 소프트웨어 디바이스가 **Panorama**에 등록할 때 콘텐츠 자동 푸시를 선택(활성화)합니다.

   이 설정은 VM 시리즈 및 CN 시리즈 방화벽에 대해서만 지원됩니다. 관리 인터페이스(**Panorama** > 설정 > 인터페이스 > 관리)에 Panorama 공용 **IP** 주소를 추가하여 바이러스 백신 및 애플리케이션 및 위협 콘텐츠 버전을 VM 시리즈 및 CN 시리즈 방화벽에 자동으로 푸시해야 합니다.

   NSX 및 하드웨어 방화벽에 배포된 *VM* 시리즈 방화벽은 지원되지 않습니다.

   Panorama에 처음 연결할 때 Panorama에 설치된 바이러스 백신, 응용 프로그램 및 위협 콘텐츠 버전을 VM 시리즈 및 CN 시리즈 방화벽에 자동으로 푸시하려면 이 설정을 활성화하십시오. Panorama는 설치된 동적 콘텐츠 버전을 한 번만 푸시하려고 시도하고 어떤 이유로든 초기 푸시가 실패하는 경우 설치된 안티바이러스 및 애플리케이션 및 위협 콘텐츠 버전의 후속 푸시를 시도하지 않습니다.

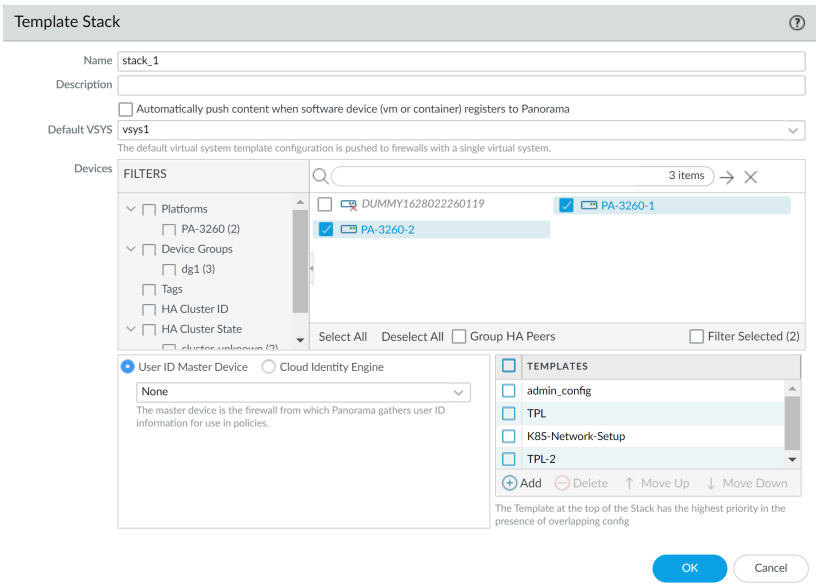
   예를 들어 Panorama 관리에 VM 시리즈 방화벽을 추가하고 첫 번째 연결 시 자동 푸시를 활성화하여 첫 번째 연결 시 디바이스 그룹 및 템플릿 스택 구성을 VM 시리즈 방화벽에 자동으로 푸시합니다. 그러나 템플릿 스택에 잘못된 구성이 포함되어 있어 VM 시리즈 방화벽에 대한 푸시가 실패합니다. 이 시나리오에서는 구성 푸시 및 동적 콘텐츠 버전 푸시가 VM 시리즈 방화벽에 대

 ©2024 Palo Alto Networks, Inc.

한 동일한 푸시 작업에 포함되어 있기 때문에 VM 시리즈 방화벽에 대한 자동 콘텐츠 푸시도 실패합니다.

자동 크기 조정을 활용할 때 이 설정을 활성화하면 정책 및 *AppID*와 같은 구성에서 동적 콘텐츠를 활용하는 *VM* 시리즈 및 *CN* 시리즈 방화벽에 대한 기존 이미지를 유지할 수 있습니다. 이는 새로운 동적 콘텐츠 업데이트 버전이 도입될 때 *VM* 시리즈 및 *CN* 시리즈 방화벽 이미지를 업데이트하는 데 필요한 운영 오버헤드를 제거하는 데 도움이 됩니다.

5. 각 템플릿에 대해 스택이 결합되고(최대 8개) 추가하고 템플릿을 선택합니다. 대화 상자는 중복 설정과 관련하여 우선 순위에 따라 추가된 템플릿을 나열합니다. 여기서 상위 템플릿의 값은 목록의 하위 템플릿보다 우선합니다. 순서를 변경하려면 템플릿을 선택하고 위로 이동 또는 아래로 이동을 선택합니다.



6. 디바이스 섹션에서 방화벽을 선택하여 스택에 할당합니다. 여러 가상 시스템이 있는 방화벽의 경우 개별 가상 시스템을 할당할 수 없으며 전체 방화벽만 할당할 수 있습니다. 모든 방화벽을 하나의 템플릿 스택에만 할당할 수 있습니다.

새 관리형 방화벽을 *Panorama*에 추가할 때마다 적절한 템플릿 스택에 할당해야 합니다. *Panorama*는 템플릿 또는 템플릿 스택에 새 방화벽을 자동으로 할당하지 않습니다. 구성 변경 사항을 템플릿에 푸시하면 *Panorama*는 템플릿 스택에 할당된 모든 방화벽에 구성을 푸시합니다.

7. (선택 사항) 고가용성(HA) 구성에 있는 방화벽에 대한 단일 확인란을 표시하려면 **Group HA Peers**를 선택합니다. 아이콘은 HA 상태를 나타냅니다. 녹색은 활성, 노란색은 수동입니다. 보조 피어의 방화벽 이름은 괄호 안에 있습니다.

   활성/수동 HA의 경우 두 피어가 모두 구성을 수신하도록 동일한 템플릿에 두 피어를 추가합니다. 활성/활성 HA의 경우 두 피어를 동일한 템플릿에 추가할지의 여부는 각 피어에 동일한 구성이 필요한지의 여부에 따라 다릅니다. PAN-OS가 HA 피어 간에 동기화하는 구성 목록은 고가용성 동기화를 참조하세요.

8. 확인을 클릭하여 템플릿 스택을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 3 | (선택 사항) 템플릿 또는 템플릿 스택 변수를 구성합니다.

STEP 4 | 필요에 따라 네트워크 및 디바이스 설정을 편집합니다.

> *vsys* 이름 바꾸기는 로컬 방화벽에서만 허용됩니다. *Panorama*에서 *vsys*의 이름을 변경하면 결과는 완전히 새로운 *vsys*가 되거나 새 *vsys* 이름이 방화벽의 잘못된 *vsys*에 매핑됩니다.

개별 방화벽 컨텍스트에서 템플릿에서 푸시된 설정을 재정의하는 것과 동일한 방식으로 Panorama가 스택에서 푸시하는 설정을 재정의할 수 있습니다. 템플릿 또는 템플릿 스택 값 재정의를 참조하십시오.

1. 편집하려는 모드별 설정만 표시하도록 탭을 필터링합니다.

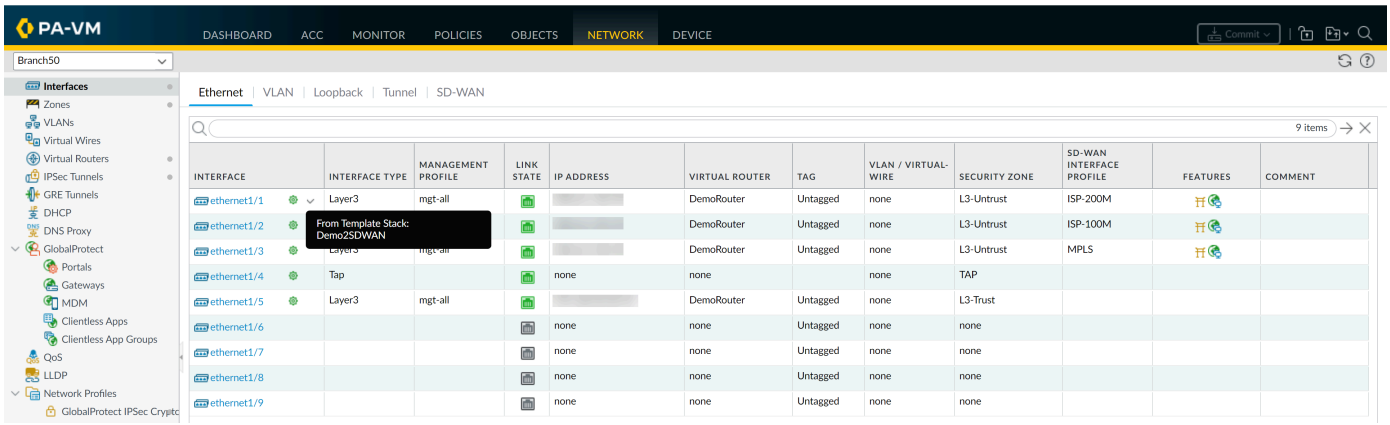
   > *Panorama*는 모드별 설정을 해당 모드를 지원하는 방화벽에만 푸시하지만 이 선택적 푸시는 모드별 값을 조정하지 않습니다. 예를 들어 템플릿에 *FIPS(Federal Information Processing Standards)* 모드의 방화벽이 있고 비 *FIPS* 알고리즘을 사용하는 *IKE Crypto* 프로파일이 있는 경우 템플릿 푸시가 실패합니다. 이러한 오류를 방지하려면 네트워크 및 디바이스 탭의 모드 드롭다운을 사용하여 모드별 기능 및 값 옵션을 필터링하십시오.

   - 모드 드롭다운에서 **Multi-VSYS**, 작동 모드 및 **VPN** 모드 필터 옵션을 선택하거나 선택 취소합니다.
   - 디바이스 드롭다운에서 선택하여 특정 방화벽의 모드 구성을 반영하도록 모든 모드 옵션을 설정합니다.
2. 인터페이스 및 네트워크 연결을 설정합니다. 예를 들어, 영역 및 인터페이스를 구성하여 네트워크를 분할하여 방화벽을 통과하는 트래픽을 관리하고 제어합니다.
3. 필요에 따라 설정을 편집합니다.
4. 커밋 > 커밋 및 푸시, 푸시 범위에서 선택 편집, 템플릿을 선택하고 템플릿 스택에 할당된 방화벽을 선택한 다음 Panorama 구성 및 템플릿 스택에 대한 변경 사항을 커밋 및 푸시합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 템플릿 스택이 예상대로 작동하는지 확인합니다.

1. 컨텍스트 드롭다운에서 템플릿 스택에 할당된 디바이스를 선택합니다.
2. 템플릿 스택을 사용하여 구성 변경 사항을 푸시한 탭을 선택합니다.
3. 템플릿 스택에서 푸시된 값에는 템플릿 아이콘( )이 표시되어 섹션의 설정에 템플릿 스택에서 푸시된 값이 있음을 나타냅니다. 스택 위로 마우스를 가져가면 값이 푸시된 템플릿 스택(template stack)을 볼 수 있습니다.



STEP 6 | 방화벽이 네트워크 리소스에 액세스할 수 있는지 확인하기 위해 네트워크 리소스에 대한 연결 문제 해결을(를) 수행합니다.

템플릿 또는 템플릿 스택(template stack) 변수 구성

템플릿 및 템플릿 스택(template stack) 변수를 사용하여 구성의 IP 주소, IP 범위, FQDN, IKE와 VPN의 인터페이스, 그룹 ID를 대체할 수 있습니다. 템플릿 스택(template stack)의 여러 템플릿이 동일한 구성 개체에 대해 서로 다른 변수를 사용하는 경우 템플릿 스택(template stack)에 의해 상속되는 변수 값은 템플릿 및 템플릿 스택(template stack)에 설명된 상속 순서를 기반으로 합니다. 또한 템플릿 스택(template stack) 변수를 사용하여 템플릿 값을 재정의하여 템플릿 스택(template stack)에서 구성 개체를 관리할 수 있습니다.

변수를 사용하면 관리해야 하는 템플릿 및 템플릿 스택(template stack)의 총 수를 줄이는 동시에 방화벽 또는 어플라이언스별 값을 유지할 수 있습니다. 예를 들어 기본 구성이 있는 템플릿 스택(template stack)이 있는 경우 변수를 사용하여 템플릿 또는 템플릿 스택(template stack)의 모든 방화벽에 적용되지 않는 값을 생성할 수 있습니다. 이를 통해 새로운 템플릿 또는 템플릿 스택(template stack)을 생성하기 전에 필요한 방화벽 또는 어플라이언스 특정 값을 고려하면서 더 적은 수의 템플릿 및 템플릿 스택(template stack)에서 구성을 관리하고 푸시할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 템플릿 및 템플릿 스택(template stack)을 생성합니다.

1. 템플릿 추가
2. 템플릿 스택 구성

STEP 3 | **Panorama** > 템플릿을 선택하고 변수를 생성하려는 템플릿 및 템플릿 스택(template stack)을 관리(변수 열)합니다.

©2024 Palo Alto Networks, Inc.

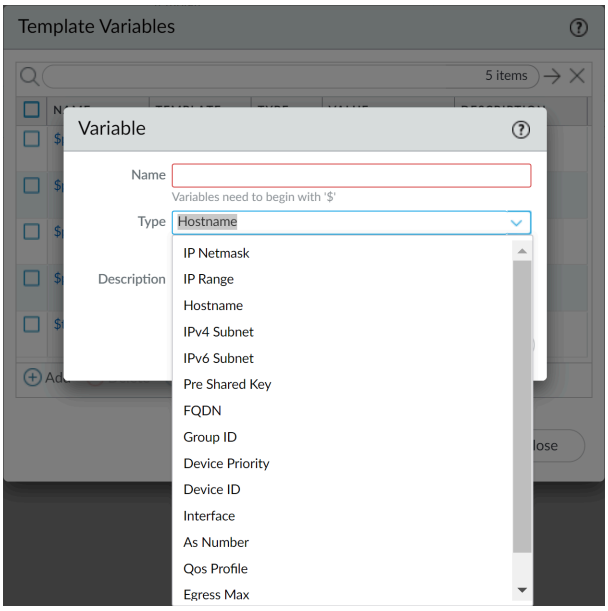
STEP 4 | 새 변수를 추가합니다.

변수 이름은 달러($) 기호로 시작해야 합니다.

1. 새 변수의 이름을 지정합니다. 이 예에서 변수의 이름은 `$DNS-primary` 및 `$DNS-secondary`입니다.
2. 변수 유형을 선택한 다음 선택한 변수 유형에 해당하는 값을 입력합니다.

   이 예에서는 **IP** 넷마스크를 선택합니다.
3. (선택 사항) 변수에 대한 설명을 입력합니다.
4. 확인 및 닫기를 클릭합니다.

변수가 지원되는 인라인에서도 변수를 생성할 수 있습니다.

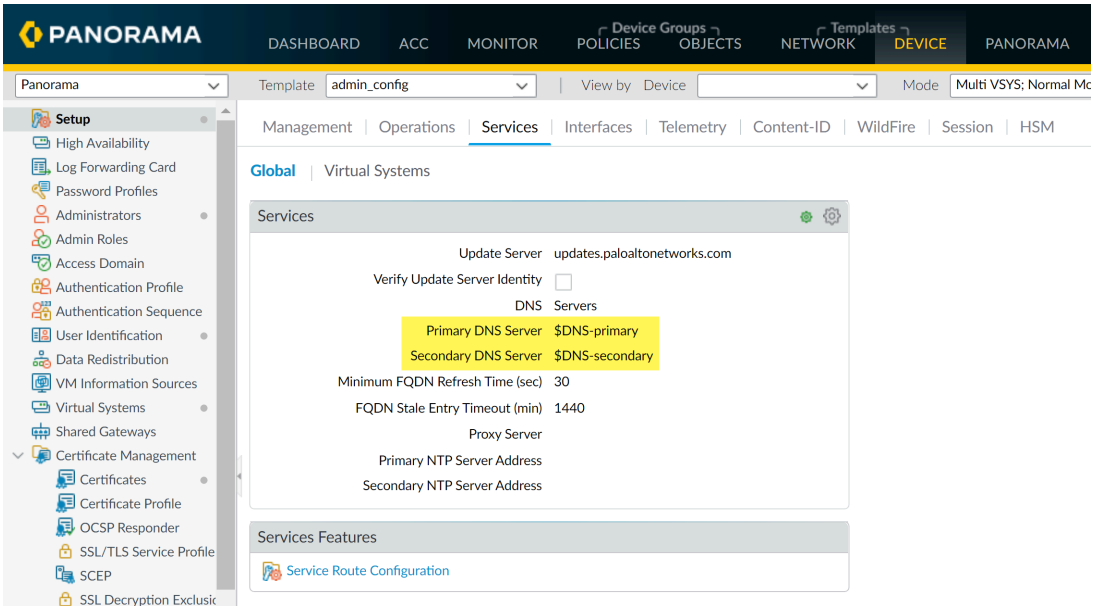


 ©2024 Palo Alto Networks, Inc.

STEP 5 | 적절한 위치에 변수를 입력합니다.

이 예에서는 이전에 정의한 DNS 값을 참조하십시오.

1. 디바이스를 선택합니다.
2. 템플릿 드롭다운에서 변수가 속한 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
3. 설정 > 서비스를 선택합니다.
4. 서비스를 편집합니다.
5. **$DNS-primary**를 입력하거나 기본 **DNS** 서버의 드롭다운에서 선택합니다.
6. **$DNS-secondary**를 입력하거나 보조 **DNS** 서버의 드롭다운에서 선택합니다.
7. 확인을 클릭합니다.



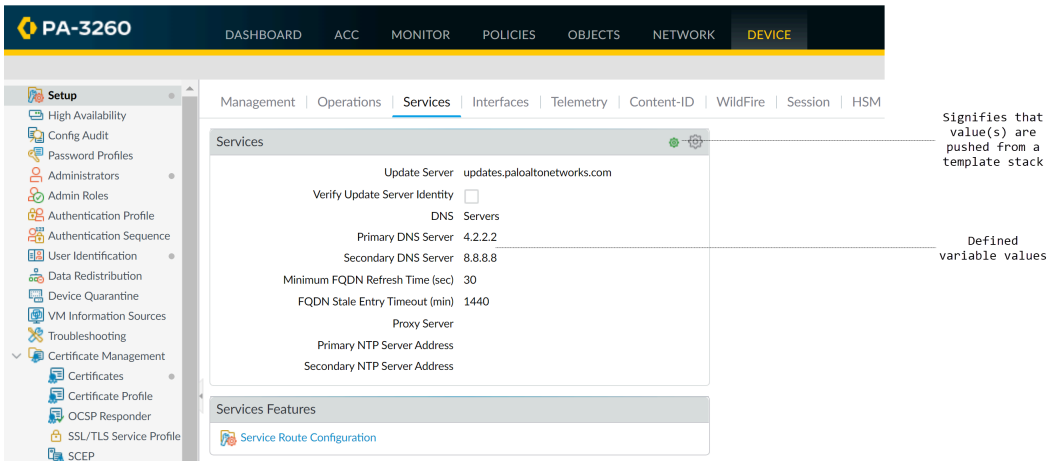
STEP 6 | 커밋 및 커밋 및 푸시를 클릭하고 관리형 방화벽에 변경 사항을 푸시합니다.

템플릿 또는 템플릿 스택*(template stack)* 변수에 대한 참조가 있는 디바이스 그룹 구성을 푸시하는 경우 선택 사항을 편집하고 디바이스 및 네트워크 템플릿을 포함해야 합니다.

©2024 Palo Alto Networks, Inc.

STEP 7 | 모든 변수의 값이 관리되는 디바이스로 푸시되었는지 확인하십시오.

1. 컨텍스트 드롭다운에서 변수가 생성된 템플릿 스택에 속한 방화벽을 선택합니다.
2. 디바이스 > 설정 > 서비스를 선택합니다.
3. 템플릿 또는 템플릿 스택에 의해 정의된 값이 있는 설정은 템플릿 기호( )로 표시됩니다. 지표 위로 마우스를 가져가면 변수 정의가 속한 템플릿 또는 템플릿 스택(template stack)을 볼 수 있습니다. 방화벽 컨텍스트에서 볼 때 변수는 변수에 대해 구성한 IP 주소로 표시됩니다.



STEP 8 | 방화벽이 네트워크 리소스에 액세스할 수 있는지 확인하기 위해 네트워크 리소스에 대한 연결 문제 해결을(를) 수행합니다.

기존 템플릿 스택(template stack) 변수 가져오기 및 덮어쓰기

템플릿 스택(template stack) 변수를 사용하여 방화벽 구성에서 IP 주소, IP 범위, FQDN, 인터페이스 또는 그룹 ID를 바꿉니다. 변수를 사용하면 관리해야 하는 템플릿과 템플릿 스택(template stack)의 총 수를 줄이는 동시에 방화벽별 값을 유지할 수 있습니다.

템플릿 스택(template stack) 변수를 가져오면 여러 기존 변수의 값을 덮어쓸 수 있으며 가져올 때 새 템플릿 스택(template stack) 변수를 만들 수 없습니다. 새 템플릿 또는 템플릿 스택(template stack) 변수를 만드는 방법에 대한 자세한 내용은 템플릿 또는 템플릿 스택(template stack) 변수 구성을(를) 참조하십시오.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 기존 템플릿 스택(template stack) 변수를 내보냅니다.

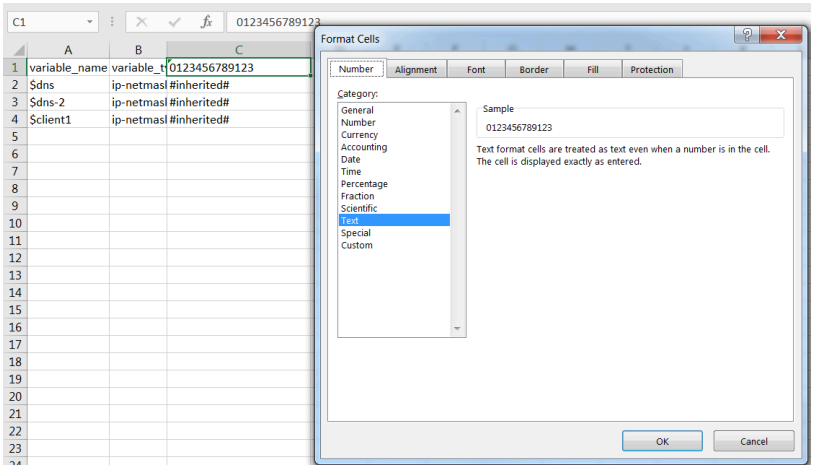
1. **Panorama** > 템플릿을 선택한 다음 템플릿 또는 템플릿 스택을 선택합니다.
2. 가변 **CSV** > 내보내기를 선택합니다. 구성된 템플릿 스택 변수는 CSV 파일로 로컬에 다운로드됩니다.
3. 내보낸 CSV를 엽니다.

 ©2024 Palo Alto Networks, Inc.

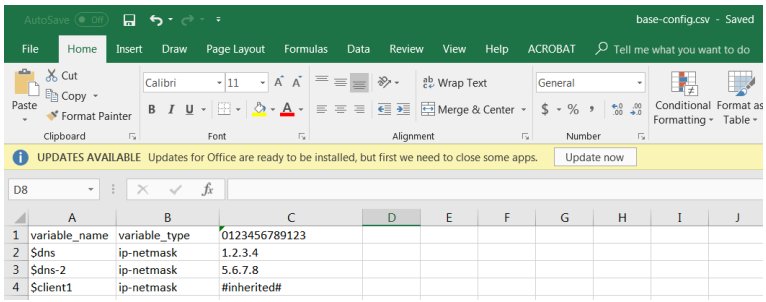
STEP 3 | Panorama로 가져올 템플릿 스택(template stack) 변수가 포함된 CSV 파일을 다음 형식으로 편집합니다.

`#inherited#`으로 표시되는 값은 템플릿 스택(template stack)에 정의된 값입니다.

1. 방화벽 일련번호가 포함된 셀의 번호를 수정합니다. CSV 파일의 모든 방화벽에 대해 이 단계를 반복합니다.
   1. 방화벽 일련번호가 포함된 셀을 마우스 오른쪽 단추로 클릭하고 셀 서식을 선택합니다.
   2. 숫자 > 텍스트를 선택한 다음 확인을 클릭합니다.
   3. 일련번호 시작 부분에 **0**을 추가합니다.



2. 원하는 템플릿 변수의 새 값을 입력합니다.
3. **File** > 다른 이름으로 저장을 선택한 다음 파일을 **CSV UTF-8** 형식으로 저장합니다.



STEP 4 | CSV 파일을 템플릿 스택으로 가져옵니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 템플릿을 선택한 다음 2단계에서 변수를 내보낸 템플릿 스택을 선택합니다.
3. 3단계에서 편집한 CSV 파일에 대해 가변 **CSV** > 가져오기 및 찾아보기를 선택합니다.
4. 확인을 클릭하여 템플릿 스택 변수를 가져옵니다.

STEP 5 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

STEP 6 | 적절한 위치에 변수를 입력합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 커밋 및 커밋 및 푸시를 클릭하고 관리형 방화벽에 변경 사항을 푸시합니다.

템플릿 또는 템플릿 스택*(template stack)* 변수에 대한 참조가 있는 디바이스 그룹 구성을 푸시하는 경우 선택 사항을 편집하고 디바이스 및 네트워크 템플릿을 포함해야 합니다.

템플릿 또는 템플릿 스택(template stack) 값 재정의

템플릿 및 템플릿 스택(template stack)을 사용하면 기본 구성을 여러 방화벽에 적용할 수 있지만 템플릿 또는 템플릿 스택(template stack)의 모든 방화벽에 적용되지 않는 방화벽별 설정을 구성할 수 있습니다. 반대로 모든 관리 방화벽에 기본 구성으로 적용할 수 있는 템플릿 스택(template stack) 구성을 생성하기 위해 템플릿 설정을 재정의할 수 있습니다. 재정의는 구성 요구 사항을 충족하기 위해 예외 또는 수정을 허용합니다. 예를 들어 템플릿을 사용하여 기본 구성을 생성하지만 테스트 랩 환경의 일부 방화벽에서 DNS(Domain Name System) 서버 IP 주소 또는 NTP(Network Time Protocol) 서버에 대해 다른 설정이 필요한 경우, 템플릿 및 템플릿 스택(template stack) 설정을 재정의할 수 있습니다.

단일 값을 재정의하는 대신 방화벽의 모든 템플릿 또는 스택 설정을 비활성화하거나 제거하려면 템플릿 설정 비활성화/제거를 참조하십시오.

다음 방법 중 하나로 템플릿 또는 템플릿 스택(template stack) 값을 재정의할 수 있습니다.

- 방화벽에서 템플릿 값 재정의 또는 변수를 사용하여 템플릿 또는 템플릿 스택(template stack) 값 재정의 - 템플릿 또는 템플릿 스택(template stack)에서 푸시된 값을 재정의하는 두 가지 방법이 있습니다. 첫 번째는 템플릿 또는 템플릿 스택(template stack)에서 푸시된 값을 재정의하기 위해 방화벽에서 로컬로 값을 정의하는 것입니다. 두 번째는 템플릿 또는 템플릿 스택(template stack)에서 푸시된 값을 재정의하기 위해 방화벽 관련 변수를 정의하는 것입니다.
- 템플릿 스택(template stack)을 사용하여 템플릿 값 재정의 - 템플릿 스택(template stack)에서 값 또는 변수를 정의하여 템플릿에서 푸시된 값을 재정의합니다.

방화벽에서 템플릿 값 재정의

템플릿 또는 템플릿 스택(template stack)에서 푸시된 로컬 방화벽의 설정을 재정의하여 방화벽별 구성을 생성합니다. 이를 통해 Panorama™에서 기본 템플릿 또는 템플릿 스택(template stack) 구성을 관리하는 동시에 다른 방화벽에는 적용되지 않는 방화벽별 구성을 유지할 수 있습니다.

STEP 1 | 방화벽 웹 인터페이스에 액세스합니다.

브라우저의 URL 필드에 IP 주소를 입력하여 방화벽에 직접 액세스하거나 Panorama의 컨텍스트 드롭다운을 사용하여 방화벽 컨텍스트로 전환합니다.

STEP 2 | 템플릿 또는 템플릿 스택(template stack)에서 푸시된 값을 재정의합니다.

이 예에서는 템플릿 추가에서 템플릿을 사용하여 할당한 DNS 서버 IP 주소를 재정의합니다.

1. 디바이스 > 설정 > 서비스를 선택한 다음 서비스 섹션을 편집합니다.
2. 기본 **DNS** 서버의 템플릿 아이콘( )을 클릭하여 해당 필드에 대한 재정의를 활성화합니다.
3. 기본 **DNS** 서버의 새 IP 주소를 입력합니다. 템플릿 재정의 기호( )는 템플릿 값이 재정의되었음을 나타냅니다.
4. 확인을 클릭하고 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

템플릿 스택(template stack)을 사용하여 템플릿 값 재정의

템플릿 스택(template stack) 값을 사용하여 템플릿에서 관리형 방화벽으로 푸시된 구성을 재정의하여 Panorama™에서 관리형 방화벽의 기본 구성을 관리하는 데 사용할 수 있는 템플릿 스택(template stack) 구성을 생성할 수 있습니다. 이를 통해 Panorama의 관리 기능을 활용하여 단일 위치에서 여러 디바이스에 구성 변경 사항을 푸시할 수 있습니다. 이 예에서는 템플릿 스택(template stack)을 사용하여 템플릿에서 푸시된 $DNS라는 기본 DNS 서버 IP 주소 변수를 재정의합니다.

*Panorama*는 템플릿 스택*(template stack)*을 사용하여 집계 인터페이스의 *Layer2* 하위 인터페이스를 제외하고 템플릿에 구성된 인터페이스를 재정의할 수 있도록 지원합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 템플릿 드롭다운에서 템플릿 구성을 재정의할 템플릿 스택을 선택합니다.

STEP 3 | 푸시된 템플릿 구성을 재정의합니다.

1. 디바이스 > 설정 > 서비스를 선택한 다음 서비스 섹션을 편집합니다.
2. 푸시된 템플릿 구성을 재정의하도록 IP 주소로 기본 **DNS**를 구성하고 확인을 클릭합니다.

STEP 4 | 구성 변경을 커밋하고 푸시합니다.

템플릿 스택(template stack) 변수를 사용하여 템플릿 값 재정의

템플릿 스택(template stack) 값과 변수를 사용하여 템플릿에서 관리형 방화벽으로 푸시된 구성을 재정의하여 Panorama™에서 관리형 방화벽의 기본 구성을 관리하는 데 사용할 수 있는 템플릿 스택(template stack) 구성을 생성할 수 있습니다. 이를 통해 Panorama의 관리 기능을 활용하여 단일 위치에서 여러 방화벽으로 구성 변경 사항을 푸시할 수 있습니다. 이 예에서는 템플릿에서 푸시된 $DNS라는 기본 DNS 서버 IP 주소 변수를 재정의하여 템플릿 스택(template stack) 변수를 생성합니다.

*Panorama*는 템플릿 스택*(template stack)*을 사용하여 집계 인터페이스의 *Layer2* 하위 인터페이스를 제외하고 템플릿에 구성된 인터페이스를 재정의할 수 있도록 지원합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 템플릿 변수를 재정의합니다.

1. **Panorama** > 템플릿을 선택합니다.
2. 재정의해야 하는 템플릿 변수가 포함된 템플릿 스택(변수 열)을 관리합니다.
3. **$DNS** 변수를 찾아 선택합니다.
4. 재정의를 선택합니다.
5. 새 변수 값을 입력하고 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋하고 푸시합니다.

변수를 사용하여 템플릿 또는 템플릿 스택(template stack) 값 재정의

방화벽별 변수를 사용하여 템플릿 또는 템플릿 스택(template stack)에서 관리형 방화벽으로 푸시된 변수를 재정의하여 방화벽별 구성을 생성할 수 있습니다. 이를 통해 Panorama™에서 다른 방화벽에 적용되지 않는 방화벽별 구성을 유지하면서 기본 템플릿 또는 템플릿 스택(template stack) 구성을 관리할 수 있습

 ©2024 Palo Alto Networks, Inc.

니다. 이를 통해 개별 방화벽에 필요한 특정 구성을 고려하면서 Panorama의 관리 기능을 활용할 수 있습니다. 이 예에서는 템플릿에서 푸시된 $DNS라는 기본 DNS 서버 IP 주소 변수를 재정의하여 방화벽 관련 변수를 생성합니다.

재정의되지 않은 템플릿 또는 템플릿 스택*(template stack)* 변수를 재정의할 수 있습니다. 템플릿 또는 템플릿 스택*(template stack)* 변수가 이미 재정의된 경우 재정의를 되돌려 방화벽 관련 변수를 생성합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 템플릿 또는 템플릿 스택(template stack) 변수를 재정의합니다.

1. **Panorama** > 관리형 디바이스 > 요약을 선택합니다.
2. 재정의해야 하는 변수가 포함된 방화벽을 편집(변수 열)합니다.
3. **$DNS** 변수를 찾아 선택합니다.
4. 재정의를 선택합니다.
5. 새 방화벽별 IP 주소를 입력하고 확인을 클릭합니다.

STEP 3 | 변경 사항을 커밋하고 푸시합니다.

템플릿 설정 비활성화/제거

관리형 방화벽에서 구성을 관리하기 위해 템플릿 또는 템플릿 스택(template stack) 사용을 중지하려는 경우 템플릿 또는 스택을 비활성화할 수 있습니다. 비활성화하면 템플릿/스택 값을 방화벽의 로컬 구성에 복사하거나 값을 삭제할 수 있습니다.

모든 템플릿 또는 스택 설정을 비활성화하거나 제거하는 대신 단일 설정을 재정의하려면 템플릿 설정 재정의를 참조하십시오.

방화벽 관리에 사용하는 방법에 대한 자세한 내용은 템플릿 및 템플릿 스택(template stack)을 참조하십시오.

STEP 1 | 운용 관리자 역할이 있는 관리자로 관리 방화벽의 웹 인터페이스에 액세스합니다. 브라우저 URL 필드에 IP 주소를 입력하거나 Panorama의 컨텍스트 드롭다운에서 방화벽을 선택하여 방화벽에 직접 액세스할 수 있습니다.

STEP 2 | 디바이스 > 설정 > 관리를 선택한 다음 Panorama 설정을 편집합니다.

STEP 3 | 디바이스 및 네트워크 템플릿 비활성화를 클릭합니다.

STEP 4 | (선택 사항) 비활성화하기 전에 디바이스 및 네트워크 템플릿 가져오기를 선택하여 구성 설정을 방화벽에 로컬로 저장합니다. 이 옵션을 선택하지 않으면 PAN-OS가 방화벽에서 Panorama 푸시 설정을 모두 삭제합니다.

STEP 5 | 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama에서 마스터 키 관리

Panorama, 방화벽, 로그 수집기 및 WF-500 어플라이언스는 마스터 키를 사용하여 구성의 중요한 요소를 암호화하고 암호 및 구성 요소를 암호화하는 데 사용하는 기본 마스터 키가 있습니다. 표준 보안 관행의 일부로 기본 마스터 키를 교체하고 만료되기 전에 각 개별 방화벽, Log Collector, WildFire 어플라이언스 및 Panorama에서 키를 변경해야 합니다.

보안 태세를 강화하려면 Panorama 및 각 관리 방화벽에 대해 고유한 마스터 키를 구성하십시오. 고유한 마스터 키를 구성하면 손상된 마스터 키가 전체 배포의 구성 암호화를 손상시키지 않도록 할 수 있습니다. 고유한 마스터 키는 Panorama 및 관리 방화벽에 대해서만 지원됩니다. Log Collectors 및 WildFire 어플라이언스는 Panorama와 동일한 마스터 키를 공유해야 합니다. 고가용성(HA) 구성의 Panorama 또는 관리형 방화벽의 경우 마스터 키가 HA 피어 간에 동기화되지 않으므로 두 HA 피어에 대해 동일한 마스터 키를 배포해야 합니다.

마스터 키가 데이터를 암호화하는 데 사용하는 기본 암호화 알고리즘은 AES-256-CBC이며, 마스터 키는 PAN-OS 10.0 이전에 사용한 것과 동일한 알고리즘입니다. AES-256-CBC는 Panorama로 방화벽을 관리할 때 관리형 방화벽이 다른 PAN-OS 릴리즈에 있을 수 있으며 PAN-OS 10.0 이전에 출시된 PAN-OS 릴리즈의 방화벽은 AES-256-GCM을 지원하지 않기 때문에 기본 암호화 수준입니다. Panorama가 관리되는 디바이스에서 사용할 수 있는 가장 낮은 수준의 암호화를 사용해야 하는 이유입니다. 예를 들어 일부 관리되는 디바이스가 PAN-OS 10.0을 실행하고 일부는 이전 버전을 실행하는 경우 Panorama는 AES-256-CBC를 사용해야 합니다. 그러나 모든 관리되는 디바이스가 PAN-OS 10.0 이상을 실행하면 Panorama와 모든 관리되는 디바이스는 AES-256-GCM을 사용할 수 있습니다.

*Palo Alto Networks*는 마스터 키 암호화에 *AES 256-GCM* 레벨 *2*를 사용할 것을 권장합니다.

고유한 마스터 키를 구성하면 마스터 키 업데이트의 운영 부담도 완화됩니다. 관리되는 방화벽에 대해 고유한 마스터 키를 구성하면 많은 수의 관리되는 방화벽에서 마스터 키 변경을 조정할 필요 없이 각 마스터 키를 개별적으로 업데이트할 수 있습니다.

마스터 키가 만료되면 현재 마스터 키를 입력해야 새 마스터 키를 구성할 수 있습니다.

마스터 키는 복구할 수 없으므로 관리 방화벽, 로그 수집기 및 *WildFire* 어플라이언스에 배포하는 마스터 키를 추적해야 합니다. 만료될 때 현재 마스터 키를 제공할 수 없는 경우 공장 기본값으로 재설정해야 합니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | (모범 사례) 보류 중인 구성 변경 사항이 있으면 커밋 및 커밋 및 푸시를 선택합니다.

Panorama는 새 마스터 키를 사용하여 데이터를 다시 암호화해야 합니다. 모든 구성 요소가 새 마스터 키로 암호화되도록 하려면 새 마스터 키를 배포하기 전에 보류 중인 모든 변경 사항을 커밋해야 합니다.

©2024 Palo Alto Networks, Inc.

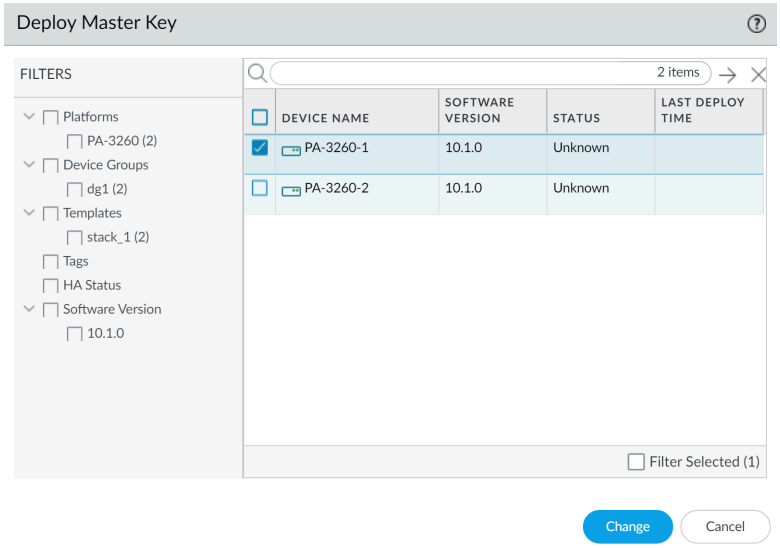
STEP 3 | 관리 방화벽에 대해 고유한 마스터 키를 구성합니다.

1. (HA에만 해당) 관리형 방화벽에 대해 구성 동기화를 사용하지 않도록 설정합니다.

   방화벽 HA 쌍에 새 마스터 키를 배포하기 전에 이 단계가 필요합니다.

   1. Panorama 웹 인터페이스에 로그인.
   2. 디바이스 > 고가용성 > 일반을 선택하고 관리형 방화벽 HA 구성을 포함하는 템플릿을 선택합니다.
   3. HA 쌍 설정 설정을 편집합니다.
   4. 구성 동기화 사용을 비활성화(지우기)하고 확인을 클릭합니다.
   5. 구성 변경 사항을 커밋 및 커밋 및 푸시를 선택합니다.
2. **Panorama** > 관리형 디바이스 > 요약을 선택한 다음 마스터 키 배포를 선택합니다.
3. 관리형 방화벽을 선택한 다음 마스터 키를 변경합니다.

   특정 관리 방화벽 집합에 대해 고유한 마스터 키를 배포하려는 경우 해당 특정 관리 방화벽도 선택할 수 있습니다.

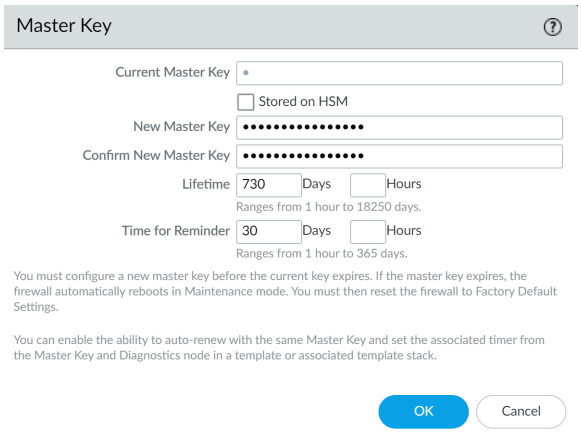


4. 마스터 키 구성:

   1. 마스터 키를 갱신하는 경우 현재 마스터 키를 입력합니다. 기본 마스터 키를 새 마스터 키로 바꾸는 경우 현재 마스터 키를 지정하지 마십시오.
   2. (선택 사항) 마스터 키가 HSM(하드웨어 보안 모듈)에서 암호화된 경우 **HSM**에 저장을 활성화(선택)합니다.
   3. 새 마스터 키를 지정하고 마스터 키를 확인합니다.
   4. 마스터 키 수명 및 미리 알림 시간을 구성합니다.
   5. 확인을 클릭합니다.

      확인을 클릭하면 새 마스터 키가 관리형 방화벽에 자동으로 푸시됩니다. 관리형 방화벽의 마스터 키를 변경할 준비가 되었다고 확신하는 경우에만 진행하십시오.

©2024 Palo Alto Networks, Inc.



5. 마스터 키가 선택한 모든 관리 방화벽에 성공적으로 배포되었는지 확인합니다.

   Panorama에서 새 마스터 키를 배포하면 시스템 로그가 생성됩니다.

6. (선택 사항) 관리형 방화벽을 자동으로 갱신하도록 마스터 키를 구성합니다.

   선택한 템플릿과 연결된 관리 방화벽에 배포된 마스터 키를 자동으로 갱신하려면 이 설정을 구성합니다. 그렇지 않으면 마스터 키는 구성된 마스터 키 수명에 따라 만료되며 새 마스터 키를 배포해야 합니다.

   1. 디바이스 > 마스터 키 및 진단을 선택한 다음 대상 관리형 방화벽이 포함된 템플릿을 선택합니다.
   2. 마스터 키 설정을 편집하고 동일한 마스터 키로 자동 갱신 설정을 구성합니다.
   3. 확인을 클릭합니다.
   4. 구성 변경 사항을 커밋 및 커밋 및 푸시를 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | Panorama에서 마스터 키를 구성합니다.

1. (HA에만 해당) Panorama에 대한 HA 구성을 사용하지 않도록 설정합니다.

   이 단계는 Panorama HA 피어 모두에 대한 마스터를 성공적으로 변경하는 데 필요합니다. Panorama가 HA 구성에 있는 경우 보조 HA 피어에서 구성 변경을 커밋할 수 없습니다.

   1. Panorama 웹 인터페이스에 로그인.
   2. **Panorama** > 고가용성 > 일반을 선택하고 HA 설정을 편집합니다.
   3. **HA** 사용을 비활성화(선택 취소)하고 확인을 클릭합니다.
   4. 커밋 및 **Panorama**에 커밋.

2. **Panorama** > 마스터 키 및 진단을 선택한 다음 마스터 키를 구성합니다.

   1. 마스터 키를 갱신하는 경우 현재 마스터 키를 입력합니다. 기본 마스터 키를 새 마스터 키로 교체하는 경우 현재 마스터 키를 지정하지 마십시오.
   2. 새 마스터 키를 구성하고 마스터 키를 확인합니다.
   3. 마스터 키 수명 및 미리 알림 시간을 구성합니다.
   4. 확인을 클릭합니다.

   > 새 마스터 키는 확인을 클릭하면 *Panorama*에 자동으로 커밋됩니다. *Panorama*에서 마스터 키를 변경할 준비가 되었다고 확신하는 경우에만 진행하십시오.

3. (선택 사항) 자동으로 갱신되도록 Panorama 마스터 키를 구성합니다.

   Panorama에 배포된 마스터 키를 자동으로 갱신하려면 이 설정을 구성합니다. 그렇지 않으면 마스터 키는 구성된 마스터 키 수명에 따라 만료되며 새 마스터 키를 배포해야 합니다.

   1. **Panorama** > 마스터 키 및 진단 을 선택한 다음 마스터 키 설정을 편집합니다.
   2. 동일한 마스터 키로 자동 갱신 설정을 구성합니다.
   3. 확인을 클릭합니다.

4. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.
5. (HA에만 해당) 이 단계를 반복하여 보조 HA 피어에서 동일한 마스터 키를 구성합니다.

   Panorama가 HA 구성에 있는 경우 기본 HA 및 보조 HA 피어에서 동일한 마스터 키를 수동으로 구성해야 합니다. 마스터 키는 기본 HA 피어와 보조 HA 피어 간에 동기화되지 않습니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 로그 수집기에 마스터 키를 배포합니다.

Log Collector에 대해 구성된 마스터 키는 Panorama에 대해 구성된 마스터 키와 동일해야 합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 마스터 키 배포를 선택합니다.
2. 모든 디바이스를 선택한 다음 마스터 키를 변경합니다.
3. 마스터 키 구성:
   1. 마스터 키를 갱신하는 경우 현재 마스터 키를 입력합니다. 기본 마스터 키를 새 마스터 키로 바꾸는 경우 현재 마스터 키를 지정하지 마십시오.
   2. 새 마스터 키를 지정하고 마스터 키를 확인합니다.
   3. 마스터 키 수명 및 미리 알림 시간을 구성합니다.
   4. 확인을 클릭합니다.

      새 마스터 키는 확인을 클릭한 후 로그 수집기로 자동으로 푸시됩니다. 로그 수집기의 마스터 키를 변경할 준비가 되었다고 확신하는 경우에만 진행하십시오.
4. 마스터 키가 선택한 모든 디바이스에 성공적으로 배포되었는지 확인합니다.

   Panorama에서 새 마스터 키를 배포하면 시스템 로그가 생성됩니다.

STEP 6 | 관리되는 WildFire 어플라이언스에 마스터 키를 배포합니다.

WildFire 어플라이언스에 구성된 마스터 키는 Panorama에 대해 구성된 마스터 키와 동일해야 합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택한 다음 마스터 키 배포를 선택합니다.
2. 모든 디바이스를 선택한 다음 마스터 키를 변경합니다.
3. 마스터 키 구성:
   1. 마스터 키를 갱신하는 경우 현재 마스터 키를 입력합니다. 기본 마스터 키를 새 마스터 키로 바꾸는 경우 현재 마스터 키를 지정하지 마십시오.
   2. 새 마스터 키를 지정하고 마스터 키를 확인합니다.
   3. 마스터 키 수명 및 미리 알림 시간을 구성합니다.
   4. 확인을 클릭합니다.

      새 마스터 키는 확인을 클릭하면 *WildFire* 어플라이언스에 자동으로 푸시됩니다. *WildFire* 어플라이언스의 마스터 키를 변경할 준비가 되었다고 확신하는 경우에만 진행하십시오.
4. 마스터 키가 선택한 모든 디바이스에 성공적으로 배포되었는지 확인합니다.

   Panorama에서 새 마스터 키를 배포하면 시스템 로그가 생성됩니다.

STEP 7 | (HA Panorama만 해당) Panorama HA 구성을 다시 구성합니다.

기본 및 보조 Panorama HA 피어 모두에 대해 이 단계를 반복합니다.

1. **Panorama** > 고가용성 > 일반을 선택하고 HA 설정을 편집합니다.
2. **HA** 활성화를 활성화(선택)하고 확인을 클릭합니다.
3. 커밋 및 **Panorama**에 커밋.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | (HA 방화벽에만 해당) 관리형 방화벽에 대해 구성 동기화를 사용하도록 설정합니다.

1. 디바이스 > 고가용성 > 일반을 선택하고 관리형 방화벽 HA 구성을 포함하는 템플릿을 선택합니다.
2. HA 쌍 설정 설정을 편집합니다.
3. 구성 동기화 사용을 활성화(선택)하고 확인을 클릭합니다.
4. 구성 변경 사항을 커밋 및 커밋 및 푸시를 선택합니다.

©2024 Palo Alto Networks, Inc.

관리되는 방화벽에 대한 구성 푸시 예약

지정된 날짜와 시간에 관리 방화벽에 변경 사항을 자동으로 푸시하도록 예약된 구성 푸시를 생성하여 관리 방화벽에 구성 변경 사항을 푸시하는 운영 오버헤드를 줄입니다. 한 번 또는 정기적으로 발생하는 일정에 따라 발생하도록 예약된 구성 푸시를 구성할 수 있습니다. 이를 통해 관리자의 개입 없이 여러 관리자가 만든 구성을 여러 방화벽에 푸시할 수 있습니다. 모든 PAN-OS 릴리스를 실행하는 대상 관리 방화벽에 대해 예약된 구성 푸시가 지원됩니다.

적절하게 정의된 관리자 역할 프로파일이 있는 운용 관리자 및 사용자 지정 Panorama 관리자는 관리되는 방화벽에 대한 예약된 구성 푸시를 생성할 수 있습니다. 예약된 구성 푸시를 생성하려면 푸시가 발생하는 시기와 빈도 및 푸시할 관리되는 방화벽에 대한 일정 매개변수를 설정합니다. 고가용성(HA) 구성의 Panorama의 경우 예약된 구성 푸시가 HA 피어 간에 동기화됩니다.

예약된 구성 푸시를 여러 개 생성하는 경우 *Panorama* 관리 서버가 구성을 검증할 수 있도록 최소 *5*분 간격으로 생성해야 합니다. 서로 *5*분 이내의 예약된 구성 푸시는 *Panorama*가 첫 번째 예약된 구성 푸시 변경 사항을 검증할 수 없기 때문에 실패할 수 있습니다.

디바이스 그룹 또는 템플릿의 마지막 커밋 상태가 ##### ## 경우 Panorama는 예약된 디바이스 그룹 및 템플릿 구성 푸시를 관리형 방화벽으로 수행합니다. 예약된 구성 푸시가 성공한 후 예약된 구성 푸시 실행 기록을 보고 특정 일정에 대한 마지막 푸시가 발생한 시간과 영향을 받은 관리되는 방화벽의 수를 이해할 수 있습니다. 영향을 받는 관리 방화벽의 총 수에서 관리 방화벽에 성공한 구성 푸시 수와 실패한 구성 푸시 수를 볼 수 있습니다. 실패한 푸시 중에서 관리형 방화벽과 Panorama 간의 연결을 중단시킨 구성 변경으로 인해 자동으로 되돌려진 구성으로 관리형 방화벽의 총 수를 볼 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 예약된 구성 푸시를 생성합니다.

1. **Panorama** > 예약된 구성 푸시를 선택한 다음 새 예약된 구성 푸시를 추가합니다.

   디바이스에 푸시할 때 관리 방화벽에 대한 구성 푸시를 예약할 수도 있습니다(디바이스에 > 푸시 커밋).

2. 예약된 구성 푸시의 이름과 빈도를 구성합니다.
   - 이름 - 구성 푸시 일정의 이름입니다.
   - 관리 범위 - 구성 변경 사항을 푸시할 관리자입니다.

     예약된 구성 푸시를 생성하는 로그인한 관리자의 이름이 기본적으로 표시됩니다. 관리자 이름을 클릭하여 예약된 구성 푸시에 Panorama 관리자를 더 추가합니다.
   - 날짜 - 구성 푸시가 다음에 발생하도록 예약된 날짜입니다.
   - 시간 - 예약된 구성 푸시 날짜에 구성 푸시가 발생하도록 예약된 시간(`hh:mm:ss`)입니다.
   - **Recurrence**(반복) - 예약된 구성 푸시가 일회성 푸시인지 또는 반복 예약 푸시(##, ## 또는 ##)인지의 여부입니다.
3. 푸시 범위 선택에서 하나 이상의 디바이스 그룹, 템플릿 또는 템플릿 스택을 선택합니다.

   구성 푸시를 성공적으로 예약하려면 하나 이상의 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택해야 합니다.

   선택한 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)과 연결된 모든 관리 방화벽이 예약된 구성 푸시에 포함됩니다.

   1. 푸시하도록 예약하려는 하나 이상의 디바이스 그룹을 선택합니다.
   2. 푸시하도록 예약하려는 템플릿을 하나 이상 선택합니다.

      단일 예약 구성 푸시에 대해 최대 *64*개의 템플릿이 지원됩니다.

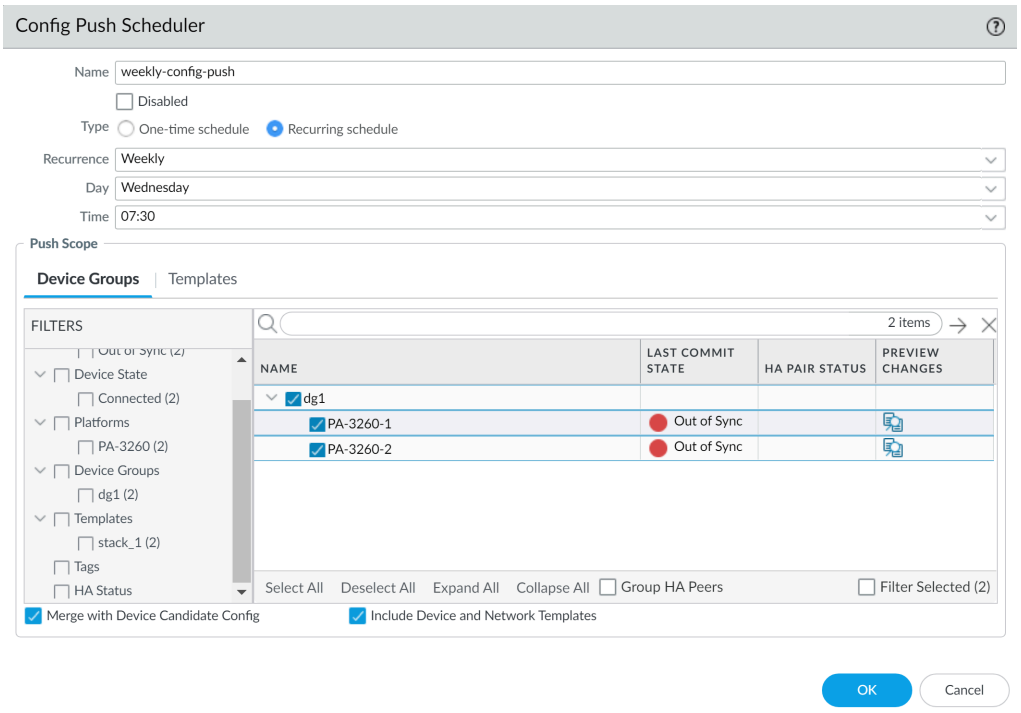
   3. Panorama에서 푸시된 구성 변경 사항을 방화벽에서 로컬로 구현된 보류 중인 구성 변경 사항과 병합하기 위해 디바이스 후보 구성과 병합할지의 여부를 확인합니다.

      이 설정은 기본적으로 활성화되어 있습니다.
   4. 단일 작업에서 디바이스 그룹 변경 사항과 관련 템플릿 변경 사항을 모두 푸시하려면 디바이스 및 네트워크 템플릿을 포함할지의 여부를 확인하십시오.

      이 설정은 기본적으로 활성화되어 있습니다. 비활성화된 경우 Panorama는 디바이스 그룹 및 관련 템플릿 변경 사항을 별도의 작업으로 푸시합니다.

      강제 템플릿 값은 로컬 방화벽 구성을 덮어쓰는 구성 푸시로 인한 업무 외 시간 중단을 방지하기 위해 예약된 구성 푸시가 지원되지 않습니다.
4. 확인을 클릭합니다.
5. 커밋 및 **Panorama**에 커밋을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.



STEP 3 | 실행 기록을 보고 모든 관리 방화벽에 대해 예약된 구성 푸시가 성공했는지 확인합니다.

1. **Panorama** > 예약된 구성 푸시를 선택한 다음 상태 열에서 마지막 실행 타임스탬프를 클릭합니다.
2. 예약된 구성 푸시에 대한 실행 기록을 봅니다.

   여기에는 예약된 구성 푸시가 마지막으로 발생한 시간과 영향을 받는 관리되는 방화벽의 총 수가 포함됩니다. 영향을 받는 총 방화벽 수 중에서 예약된 구성 푸시가 성공한 수, 실패한 수 및 Panorama에서 관리되는 방화벽 간의 연결 끊기를 유발한 구성 변경으로 인해 자동으로 구성을 되돌린 관리되는 방화벽의 수를 볼 수 있습니다.
3. 최근에 예약된 구성 푸시에 대한 전체 작업 세부 정보를 보려면 작업을 클릭합니다.

©2024 Palo Alto Networks, Inc.

관리되는 방화벽에 데이터 재분배

정책을 시행하고 보고서를 생성하는 모든 방화벽이 정책 규칙에 필요한 데이터와 인증 타임스탬프를 갖도록 하기 위해 Panorama 인프라를 활용하여 매핑과 타임스탬프를 재배포할 수 있습니다.

- 데이터를 재배포하도록 Panorama 관리 서버를 구성합니다.
  1. 방화벽, 가상 시스템 또는 Windows 사용자 ID 에이전트를 Panorama에 재배포 에이전트로 추가:
     1. **Panorama** > 데이터 재배포를 선택한 다음 각 재배포 에이전트를 추가합니다.
     2. 재배포 에이전트를 식별할 이름을 입력합니다.
     3. 에이전트가 활성화되어 있는지 확인합니다.
     4. 방화벽에 있는 MGT 인터페이스의 호스트 이름 또는 IP 주소를 입력합니다.
     5. 방화벽이 데이터 재배포 쿼리를 수신할 포트 번호를 입력합니다(기본값은 5007).
     6. 재배포 에이전트가 방화벽 또는 가상 시스템인 경우 수집기 이름과 수집기 사전 공유 키를 입력합니다.
     7. 재배포할 데이터 유형을 선택하십시오. 모든 데이터 유형을 선택할 수 있지만 다음 데이터 유형 중 하나 이상을 선택해야 합니다.
        - **IP** 사용자 매핑
        - **IP** 태그 사용자 태그
        -
        - **HIP**
        - 격리 목록
     8. 확인을 클릭하여 구성을 저장합니다.
  2. Panorama MGT 인터페이스를 활성화하여 방화벽의 데이터 재배포 쿼리에 응답합니다.

     Panorama 관리 서버에 고가용성*(HA)* 구성이 있는 경우 *Panorama*가 페일오버된 경우 재배포가 계속되도록 모범 사례로 각 *HA* 피어에서 이 단계를 수행합니다.

     1. **Panorama** > **Setup** > 인터페이스 및 관리를 선택합니다.
     2. 네트워크 서비스 섹션에서 사용자 **ID**를 선택한 다음 확인을 클릭합니다.
  3. 커밋 > **Panorama**에 커밋을 선택하여 Panorama에서 변경 사항을 활성화합니다.

©2024 Palo Alto Networks, Inc.

- Panorama가 재배포하는 데이터를 수신하도록 방화벽을 구성합니다.
  1. 데바이스 > 데이터 재배포 > 에이전트를 선택한 다음 방화벽이 할당된 템플릿을 선택합니다.
  2. 에이전트를 추가하고 이름을 입력합니다.
  3. 에이전트를 추가할 방법을 선택합니다.
     - 일련 번호 - 목록에서 사용할 Panorama의 일련 번호 선택:
       - **panorama** - 활성 또는 단독 Panorama
       - **panorama2** - (HA 전용) 수동 Panorama
     - 호스트 및 포트 - 다음 정보 지정:
       - 방화벽에서 MGT 인터페이스의 호스트 이름 또는 IP 주소를 선택합니다.
       - 호스트가 **LDAP** 프록시인지 여부를 선택합니다.
       - 방화벽이 데이터 재배포 쿼리를 수신할 포트 번호를 입력합니다(기본값은 5007).
       - 재배포 에이전트가 방화벽 또는 가상 시스템인 경우 수집기 이름 및 수집기 사전 공유 키를 입력합니다.
       - 재배포할 데이터 유형을 선택합니다.
  4. 에이전트가 활성화되었는지 확인하고 확인을 클릭하여 구성을 저장합니다.
  5. 커밋 > 커밋 및 푸시를 선택하여 Panorama에서 변경 사항을 활성화하고 방화벽으로 변경 사항을 푸시합니다.

- Panorama 및 방화벽이 재배포된 데이터를 수신하는지 확인합니다.
  1. 에이전트 통계 **Panorama** > 데이터 재배포 > 에이전트를 보고 상태를 선택하여 클라이언트 방화벽이 수신한 매핑 수와 같은 재배포 에이전트에 대한 활동 요약을 봅니다.
  2. 사용자 ID 로그에서 소스 이름(모니터 > 로그 > 사용자 **ID**을 확인하여 방화벽이 재배포 에이전트로부터 매핑을 수신하는지 확인합니다.
  3. IP 태그 로그(모니터 > 로그 > **IP** 태그)를 보고 클라이언트 방화벽이 데이터를 수신하는지 확인합니다.
  4. 데이터를 재배포하는 방화벽 또는 Panorama 관리 서버의 CLI에 액세스합니다.
  5. 다음 명령을 실행하여 모든 사용자 매핑을 표시합니다.

     ```
     > show user ip-user-mapping all
     ```

  6. 하나의 사용자 이름과 연결된 IP 주소를 기록합니다.
  7. 재배포된 데이터를 수신하는 방화벽 또는 Panorama 관리 서버의 CLI에 액세스합니다.
  8. 기록된 *<IP-address>*에 대한 매핑 정보 및 인증 타임스탬프를 표시합니다.

     ```
     > show user ip-user-mapping ip <IP-address> IP
      address:    192.0.2.0 (vsys1) User:          corpdomain
     \username1 From:          UIA ## ## ##:  ## 10229#
     ```

 ©2024 Palo Alto Networks, Inc.

```
TTL:      10229s MFA Timestamp: first(1) - 2016/12/09
08:35:04 Group(s): corpdomain\groupname(621)
```

이 예제 출력은 하나의 인증 챌린지(요소)에 대한 응답의 타임스탬프를 보여줍니다. MFA(다단계 인증)를 사용하는 인증 규칙의 경우 출력에 여러 타임스탬프가 표시됩니다.

©2024 Palo Alto Networks, Inc.

방화벽을 Panorama 관리로 전환

Palo Alto Networks 방화벽을 이미 배포하고 로컬로 구성했지만 이제 Panorama를 사용하여 방화벽을 중앙에서 관리하려는 경우 사전 마이그레이션 계획을 수행해야 합니다. 마이그레이션에는 방화벽 구성을 Panorama로 가져오고 전환 후 방화벽이 예상대로 작동하는지 확인하는 작업이 포함됩니다. 일부 설정이 개별 방화벽에 고유한 경우 방화벽에 계속 액세스하여 고유한 설정을 관리할 수 있습니다. Panorama에서 값을 푸시하거나 방화벽에서 로컬로 구성하여 주어진 방화벽 설정을 관리할 수 있지만 Panorama와 방화벽을 통해 설정을 관리할 수는 없습니다. Panorama 관리에서 특정 방화벽 설정을 제외하려면 다음 중 하나를 수행할 수 있습니다.

- 전체 방화벽 구성을 마이그레이션한 다음 Panorama에서 방화벽에서 로컬로 관리할 설정을 삭제합니다. Panorama에서 설정을 삭제하는 대신 Panorama가 방화벽으로 푸시하도록 템플릿 또는 템플릿 스택(template stack) 값 재정의을(를) 할 수도 있습니다.
- Panorama를 사용하여 관리할 설정만 포함하여 부분 방화벽 구성을 로드합니다.

> 방화벽은 *Panorama* 관리로 전환하는 동안 로그를 잃지 않습니다.

- Panorama 관리로의 전환 계획
- 방화벽을 Panorama 관리로 마이그레이션하고 기존 구성 재사용
- 방화벽을 Panorama 관리로 마이그레이션하고 새 구성 푸시
- 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성 재사용
- 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성 푸시
- 부분 방화벽 구성을 Panorama에 로드
- 관리되는 방화벽에서 Panorama 푸시 구성 현지화

Panorama 관리로의 전환 계획

다음 작업은 방화벽을 Panorama 관리로 마이그레이션하는 데 필요한 계획의 상위 수준 개요입니다.

- ☐ 마이그레이션할 방화벽을 결정합니다.
- ☐ 유지 관리 기간을 계획하고 Panorama 또는 방화벽에 보류 중인 구성 변경 사항이 없는지 확인합니다.
- ☐ 한 Panorama에서 다른 Panorama로 방화벽을 마이그레이션하는 경우 방화벽에서 Panorama 푸시 구성을 현지화합니다.
- ☐ 마이그레이션하기 전에 알려진 작동하는 Panorama 및 방화벽 구성을 유지하십시오.
  - 방화벽의 디바이스 상태를 내보냅니다.
  - 실행 중인 Panorama 구성의 명명된 Panorama 구성 스냅샷을 내보냅니다.
- ☐ Panorama 및 방화벽 소프트웨어와 콘텐츠 버전, 라이선스 및 소프트웨어 업그레이드 관리 방법을 결정합니다. 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
- ☐ 공유 설정을 관리하는 방법을 계획합니다.

  중복을 줄이고 모든 방화벽 간에 또는 방화벽 집합 내에서 공유되는 설정 관리를 간소화하는 방식으로 디바이스 그룹 계층, 템플릿 및 템플릿 스택(template stack)을(를) 계획합니다. 마이그레이션하는 동안

©2024 Palo Alto Networks, Inc.

다음 예외를 제외하고 방화벽의 공유 위치에서 Panorama의 공유로 개체를 가져올지의 여부를 선택할 수 있습니다.

- 공유 방화벽 개체가 기존 공유 Panorama 개체와 이름 및 값이 동일한 경우 가져오기에서 해당 방화벽 개체를 제외합니다.
- 공유 방화벽 개체의 이름이나 값이 기존 공유 Panorama 개체와 다른 경우 Panorama는 가져오기를 위해 생성된 각각의 새 디바이스 그룹으로 방화벽 개체를 가져옵니다.
- 템플릿으로 불러온 구성이 공유 방화벽 개체를 참조하거나 공유 방화벽 개체가 템플릿으로 불러온 구성을 참조하는 경우 Panorama는 디바이스의 공유 개체를 **Panorama**의 공유 컨텍스트로 가져오기 체크박스를 선택했는지의 여부와 관계없이 개체를 공유 개체로 가져옵니다.

- ❑ Panorama에 이미 유사한 요소가 포함되어 있거나 해당 요소가 방화벽 관련 요소(예: 시간대 설정)이기 때문에 가져오고 싶지 않고 Panorama를 통해 관리하지 않는 구성 요소(정책, 개체 및 기타 설정)가 방화벽에 있는지 확인합니다. Panorama에 유사한 요소가 있는지 확인하기 위해 전역 찾기를 수행할 수 있습니다.
- ❑ 각 디바이스 그룹에 대한 공통 영역을 결정합니다. 여기에는 각 디바이스 그룹의 방화벽 및 가상 시스템에 대한 영역 이름 지정 전략이 포함됩니다. 예를 들어 Branch LAN 및 WAN이라는 영역이 있는 경우 Panorama는 포트 또는 미디어 유형, 모델 또는 논리적 주소 지정 스키마의 변화를 인식하지 않고 해당 영역을 참조하는 정책 규칙을 푸시할 수 있습니다.
- ❑ 마이그레이션 후 테스트 계획을 생성합니다.

  테스트 계획을 사용하여 마이그레이션 후에도 방화벽이 이전처럼 효율적으로 작동하는지 확인합니다. 계획에는 다음과 같은 작업이 포함될 수 있습니다.

  - 마이그레이션 후 최소 24시간 동안 방화벽을 모니터링합니다.
  - Panorama 및 방화벽 로그에 이상이 있는지 모니터링합니다.
  - Panorama에서 관리자 로그인을 확인하십시오.
  - 여러 소스에서 다양한 유형의 트래픽을 테스트합니다. 예를 들어 대역폭 그래프, 세션 수 및 거부 규칙 트래픽 로그 항목을 확인합니다(가시성을 위해 Panorama 사용 참조). 테스트는 정책 구성의 대표적인 샘플을 다루어야 합니다.
  - 사용자가 보고한 문제에 대해서는 네트워크 운영 센터(NOC) 및 보안 운영 센터(SOC)에 문의하십시오.
  - 방화벽 기능을 확인하는 데 도움이 되는 다른 테스트 기준을 포함합니다.

방화벽을 Panorama 관리로 마이그레이션하고 기존 구성 재사용

방화벽을 Panorama 관리로 마이그레이션하고 기존 방화벽 구성을 Panorama로 가져와서 재사용합니다. 방화벽 구성을 가져오면 Panorama는 불러온 네트워크 및 디바이스 설정을 포함하는 템플릿을 자동으로 생성합니다. 불러온 정책 및 개체를 포함하기 위해 Panorama는 자동으로 각 방화벽에 대해 하나의 디바이스 그룹을 생성하거나 Multi-VSYS 방화벽에서 각 가상 시스템(vsys)에 대해 하나의 디바이스 그룹을 생성합니다.

다음 단계를 수행하면 Panorama가 전체 방화벽 구성을 가져옵니다. 또는 부분 방화벽 구성을 Panorama로 로드할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

방화벽을 Panorama 관리로 마이그레이션하고 새 구성을 만들려면 방화벽을 Panorama 관리로 마이그레이션하고 새 구성 푸시의 내용을 참조하십시오. 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하려면 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성 재사용을(를) 참조하십시오.

*Panorama*는 *PAN-OS 5.0* 이상의 버전을 실행하는 방화벽에서 구성을 가져올 수 있으며 해당 방화벽에 구성을 푸시할 수 있습니다. 예외는 *Panorama 6.1* 이상의 버전이 *PAN-OS 6.0.0 ~ 6.0.3*을 실행하는 방화벽에 구성을 푸시할 수 없다는 점입니다.

*Panorama*는 이미 관리되는 디바이스인 방화벽에서 구성을 가져올 수 있지만 디바이스 그룹이나 템플릿에 아직 할당되지 않은 경우에만 가능합니다.

STEP 1 | 마이그레이션을 계획합니다.

Panorama 관리로의 전환 계획의 체크리스트를 참조하십시오.

STEP 2 | 방화벽을 관리되는 디바이스로 추가하십시오.

Panorama 관리에 방화벽을 추가하는 방법에 대한 자세한 내용은 관리형 디바이스로 방화벽 추가를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
   디바이스 등록 인증 키를 성공적으로 생성한 후 인증 키를 복사합니다.
3. **Panorama** > 관리형 디바이스 > 요약을 선택하여 방화벽을 관리 기기로 추가합니다.
4. 방화벽의 일련번호를 입력하고 확인을 클릭합니다.

   여러 방화벽 구성을 가져올 경우 별도의 줄에 각 구성의 일련번호를 입력합니다. 선택적으로 *Microsoft Excel* 워크시트에서 일련번호를 복사하여 붙여넣을 수 있습니다.
5. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 3 | 방화벽에서 Panorama로의 연결을 설정합니다.

1. 방화벽 웹 인터페이스에 로그인
2. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
3. **Panorama Servers** 필드에 Panorama 관리 서버의 IP 주소를 입력합니다.
4. 이전 단계에서 복사한 인증 키를 붙여넣습니다.
5. 확인 및 커밋을 클릭합니다.

STEP 4 | 방화벽 구성을 Panorama로 가져옵니다.

나중에 방화벽 구성을 다시 가져오기로 결정한 경우 먼저 방화벽 디바이스 그룹과 템플릿이 구성원으로 있는 템플릿을 제거하십시오. 디바이스 그룹 및 템플릿 이름이 방화벽 호스트 이름과 동일한 경우 방화벽 구성을 다시 가져오기 전에 디바이스 그룹 및 템플릿을 삭제하거나 디바이스 그룹 이름 접두사 필드를 사용하여 다시 가져오기로 생성된 디바이스 그룹 및 템플릿의 새 이름을 정의할 수 있습니다. 또한 방화벽은 디바이스 그룹 또는 템플릿에서 제거해도 로그가 손실되지 않습니다.

©2024 Palo Alto Networks, Inc.

1. Panorama에서 **Panorama** > 설정 > 작업을 선택하고 **Panorama**로 디바이스 구성 가져오기를 클릭한 다음 디바이스를 선택합니다.

   *Panorama*는 기존 디바이스 그룹 또는 템플릿에 할당된 방화벽에서 구성을 가져올 수 없습니다.

2. (선택 사항) 템플릿 이름을 편집합니다. 기본값은 방화벽 이름입니다. 기존 템플릿 또는 템플릿 스택의 이름을 사용할 수 없습니다.
3. (선택 사항) 디바이스 그룹 이름을 편집합니다. Multi-VSYS 방화벽의 경우 각 디바이스 그룹에는 기본적으로 vsys 이름이 있으므로 각 디바이스 그룹 이름 접두사로 문자열을 추가하십시오. 그렇지 않으면 기본값은 방화벽 이름입니다. 기존 디바이스 그룹의 이름을 사용할 수 없습니다.

   디바이스의 공유 개체를 ***Panorama***의 공유 컨텍스트로 가져오기 확인란이 기본적으로 선택되어 있습니다. 즉, *Panorama*는 방화벽의 공유 위치에 속하는 가져오기 개체를 *Panorama*의 공유와 비교합니다. 불러온 개체가 방화벽의 공유 컨텍스트에 없으면 가져오는 각 디바이스 그룹에 적용됩니다. 확인란을 선택 취소하면 *Panorama* 복사본은 불러온 개체를 비교하지 않고 모든 공유 방화벽 개체를 공유 대신 가져오는 디바이스 그룹에 적용합니다. 이렇게 하면 중복 개체가 생성될 수 있으므로 대부분의 경우 확인란을 선택하는 것이 가장 좋습니다. 공유 또는 복제 개체를 *Panorama*로 가져올 때의 결과를 이해하려면 공유 설정 관리 방법 계획을 참조하십시오.
4. 불러온 정책 규칙에 대한 규칙 가져오기 위치 선택: 사전 규칙 베이스 또는 사후 규칙 베이스. 선택에 관계없이 Panorama는 기본 보안 규칙(intrazone-default 및 interzone-default)을 사후 규칙 베이스로 가져옵니다.

   *Panorama*에 가져오는 방화벽 규칙과 이름이 같은 규칙이 있는 경우 *Panorama*는 두 규칙을 모두 표시합니다. 커밋 오류를 방지하려면 *Panorama* 커밋을 수행하기 전에 규칙 중 하나를 삭제하세요.
5. 확인을 클릭합니다. Panorama는 가져오기 상태, 결과, 선택에 대한 세부 정보, 불러온 항목에 대한 세부 정보 및 경고를 표시합니다. 닫기를 클릭합니다.
6. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama에서 새로 추가된 방화벽으로 구성 번들을 푸시하여 로컬 구성에서 모든 정책 규칙 및 개체를 제거합니다.

이 단계는 다음 단계에서 Panorama에서 방화벽으로 디바이스 그룹 구성을 푸시할 때 커밋 오류를 일으킬 수 있는 중복 규칙 또는 개체 이름을 방지하는 데 필요합니다.

로컬 방화벽 구성 업데이트를 제거하기 위해 *Panorama*에서 불러온 방화벽 구성 푸시 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 새로 관리되는 방화벽에 푸시한 날짜를 반영하는 정책 규칙 생성 및 수정 날짜. 또한 각 정책 규칙에 대한 새로운 UUID(Universally Unique Identifier)가 생성됩니다.

이 단계는 방화벽 관리를 *Panorama* 관리 서버로 성공적으로 마이그레이션하는 데 필요합니다. 이 단계를 성공적으로 수행하지 못하면 구성 오류 및 커밋 실패가 발생합니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 설정 > 작업 및 디바이스 구성 번들 내보내기 또는 푸시를 선택합니다.
3. 구성을 불러온 디바이스를 선택한 다음 확인을 클릭합니다.

   마스터 키가 구성된 경우 마스터 키 사용하고 마스터 키를 입력한 후 확인을 클릭합니다.
4. 푸시 및 커밋을 선택합니다. Panorama는 번들을 푸시하고 방화벽에서 커밋을 시작합니다.
5. 푸시가 성공적으로 커밋된 후 닫기를 클릭합니다.
6. 방화벽의 웹 인터페이스를 시작하고 구성이 성공적으로 커밋되었는지 확인합니다. 그렇지 않은 경우 방화벽에서 로컬로 변경 사항을 커밋합니다.
7. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 6 | 디바이스 그룹 및 템플릿 구성을 푸시하여 중앙 집중식 관리로의 전환을 완료합니다.

이 단계는 방화벽에 구성된 모든 로컬 네트워크 및 디바이스 설정을 덮어씁니다.

여러 방화벽을 마이그레이션하는 경우 계속하기 전에 각 방화벽에 대해 이 단계를 포함하여 이전 단계를 모두 수행하십시오.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 디바이스 그룹을 선택한 다음 불러온 방화벽 구성이 포함된 디바이스 그룹을 선택합니다.
3. 디바이스 후보 구성과 병합, 디바이스 및 네트워크 템플릿 포함 및 템플릿 값 강제를 선택합니다.
4. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
5. 변경 사항을 커밋하고 푸시합니다.

STEP 7 | Panorama 웹 인터페이스에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 디바이스 그룹과 템플릿 스택(template stack)이 방화벽에 대해 동기화되어 있는지 확인합니다. 방화벽 웹 인터페이스에서 구성 개체가 Panorama에서 푸시되었음을 나타내는 녹색 톱니바퀴가 표시되는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 불러온 구성을 미세 조정합니다.

1. **Panorama** > 구성 감사를 선택한 다음 비교를 위해 실행 중 구성 및 후보 구성을 선택한 다음 실행을 클릭하고 출력을 검토합니다.
2. 가져오기 후에 Panorama가 표시한 모든 경고 및 구성 감사를 기반으로 필요에 따라 디바이스 그룹 및 템플릿 구성을 업데이트합니다. 예:
   - 중복 개체 및 정책 규칙을 삭제합니다.
   - 정책 규칙 또는 개체를 다른 디바이스 그룹으로 이동하거나 복제합니다.
   - 방화벽을 다른 디바이스 그룹 또는 템플릿으로 이동합니다.
   - Panorama가 가져오는 동안 생성한 디바이스 그룹을 다른 상위 디바이스 그룹으로 이동합니다. **Panorama** > 디바이스 그룹을 선택한 다음 이동할 디바이스 그룹을 선택한 다음 새 상위 디바이스 그룹을 선택한 다음 확인을 클릭합니다.

STEP 9 | 불러온 모든 방화벽 구성을 통합합니다.

여러 방화벽을 마이그레이션하는 경우 이 단계가 필요합니다.

1. 모든 방화벽 구성을 불러온 후 필요에 따라 디바이스 그룹과 템플릿을 업데이트하여 중복을 제거하고 구성 관리를 간소화합니다. 불러온 구성 미세 조정을 참조하십시오. (방화벽 구성 번들을 다시 푸시할 필요가 없습니다.)
2. 방화벽 관련 설정을 구성합니다.

   방화벽에 로컬 영역이 있는 경우 디바이스 그룹 또는 템플릿 커밋을 수행하기 전에 로컬 영역을 만들어야 합니다. Panorama는 영역 이름 또는 영역 구성에 대해 방화벽을 폴링할 수 없습니다. 로컬 방화벽 규칙을 사용하는 경우 해당 이름이 고유한지 확인하십시오(Panorama에서 중복되지 않음). 필요한 경우 방화벽 관련 값으로 템플릿 또는 템플릿 스택(template stack) 값 재정의할 수 있습니다.
3. 변경 사항을 커밋하고 푸시합니다.
   1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 변경한 디바이스 그룹을 선택한 다음 디바이스 및 네트워크 템플릿 포함을 선택합니다.
   3. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
   4. 변경 사항을 커밋하고 푸시합니다.

STEP 10 | 마이그레이션 후 테스트 계획을 수행합니다.

마이그레이션 계획 중에 고안한 확인 작업을 수행하여 원래 로컬 구성에서와 마찬가지로 Panorama 푸시 구성에서도 방화벽이 효율적으로 작동하는지 확인합니다. 마이그레이션 후 테스트 계획 생성을 참조하세요.

방화벽을 Panorama 관리로 마이그레이션하고 새 구성 푸시

이 절차에서는 로컬 방화벽 구성을 *Panorama*에서 푸시된 구성으로 덮어씁니다.

 ©2024 Palo Alto Networks, Inc.

방화벽을 Panorama 관리로 마이그레이션하고 디바이스 그룹 및 템플릿 스택(template stack)을 사용하여 새로운 Panorama 관리형 구성을 생성합니다.

다음 단계를 수행하면 Panorama가 전체 방화벽 구성을 가져옵니다. 또는 부분 방화벽 구성을 Panorama로 로드할 수 있습니다.

방화벽을 Panorama 관리로 마이그레이션하고 기존 구성을 재사용하려면 방화벽을 Panorama 관리로 마이그레이션하고 기존 구성 재사용의 내용을 참조하십시오. 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하려면 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성 푸시을(를) 참조하십시오.

*Panorama*는 *PAN-OS 5.0* 이상의 버전을 실행하는 방화벽에서 구성을 가져올 수 있으며 해당 방화벽에 구성을 푸시할 수 있습니다. 예외는 *Panorama 6.1* 이상의 버전이 *PAN-OS 6.0.0 ~ 6.0.3*을 실행하는 방화벽에 구성을 푸시할 수 없다는 점입니다.

*Panorama*는 이미 관리되는 디바이스인 방화벽에서 구성을 가져올 수 있지만 디바이스 그룹이나 템플릿에 아직 할당되지 않은 경우에만 가능합니다.

STEP 1 | 마이그레이션을 계획합니다.

Panorama 관리로의 전환 계획의 체크리스트를 참조하십시오.

STEP 2 | 방화벽을 관리되는 디바이스로 추가하십시오.

Panorama 관리에 방화벽을 추가하는 방법에 대한 자세한 내용은 관리형 디바이스로 방화벽 추가를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
   디바이스 등록 인증 키를 성공적으로 생성한 후 인증 키를 복사합니다.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하여 방화벽을 관리되는 디바이스로 추가합니다.
4. 방화벽의 일련번호를 입력하고 확인을 클릭합니다.

   여러 방화벽을 동시에 추가하려면 각 방화벽의 일련번호를 라인별로 입력합니다.
5. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 3 | 방화벽에서 Panorama로의 연결을 설정합니다.

1. 방화벽 웹 인터페이스에 로그인
2. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
3. **Panorama Servers** 필드에 Panorama 관리 서버의 IP 주소를 입력합니다.
4. 이전 단계에서 복사한 인증 키를 붙여넣습니다.
5. 확인 및 커밋을 클릭합니다.

STEP 4 | Panorama 웹 인터페이스에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 #### ##가 ## #인지 확인합니다.

STEP 5 | 디바이스 그룹 추가.

이 단계를 반복하여 방화벽 구성을 논리적으로 그룹화하는 데 필요한 만큼의 디바이스 그룹을 만듭니다. 디바이스 그룹은 디바이스 그룹 개체와 정책을 관리하는 데 필요합니다. 디바이스 그룹을 관리하는 방법에 대해 자세히 알아보십시오.

©2024 Palo Alto Networks, Inc.

STEP 6 | 템플릿 및 템플릿 스택(template stack)을 생성합니다.

템플릿 및 템플릿 스택(template stack)은 방화벽이 네트워크에서 작동할 수 있도록 방화벽 네트워크와 디바이스 설정을 구성하는 데 사용됩니다.

1. 템플릿 추가.

   이 단계를 반복하여 필요한 네트워킹 구성을 정의하는 데 필요한 만큼의 템플릿을 만듭니다.

2. 템플릿 스택(template stack) 구성.

   이 단계를 반복하여 정의된 네트워킹 구성을 빠르게 적용하는 데 필요한 만큼의 템플릿 스택(template stack)을 생성합니다. 템플릿 스택(template stack)을 생성할 때는 관련 템플릿과 관리형 방화벽을 할당합니다.

STEP 7 | 필요에 따라 디바이스 그룹, 템플릿 및 템플릿 스택(template stack)을 구성합니다.

STEP 8 | 디바이스 그룹 및 템플릿 구성을 푸시하여 중앙 집중식 관리로의 전환을 완료합니다.

1. 커밋 > 커밋 및 푸시를 선택합니다.
2. (선택 사항) 선택 수정을 클릭하여 푸시 범위를 수정합니다.
   - 디바이스 후보 구성과 병합 — 이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 Panorama의 구성 푸시와 병합합니다. 로컬 방화벽 구성은 Panorama에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 병합되고 커밋됩니다.

     Panorama 관리 구성과 별도로 로컬 방화벽 구성 변경 사항을 관리하고 커밋하는 경우 이 설정을 비활성화합니다.
   - 템플릿 값 강제 적용 — 값이 충돌하는 경우 모든 로컬 방화벽 구성을 Panorama에서 푸시된 템플릿 스택(template stack) 구성의 값으로 덮어씁니다.

     이 설정은 기본적으로 활성화되어 있습니다. 이 설정을 활성화하면 충돌하는 방화벽 구성을 템플릿 또는 템플릿 스택(template stack)에 정의된 값으로 덮어씁니다. 이 설정을 활성화하기 전에 재정의된 값을 검토하여 중단이 발생하지 않도록 합니다.

   확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
3. 변경 사항을 커밋하고 푸시합니다.

STEP 9 | **Panorama** > 관리되는 디바이스 > 요약을 선택하고 새로 추가된 방화벽에 대한 ## ##과 ### 상태가 ### #으로 되어 있는지 확인합니다.

방화벽 웹 인터페이스에서 구성 개체가 Panorama에서 푸시되었음을 나타내는 녹색 톱니바퀴가 표시되는지 확인합니다.

STEP 10 | 마이그레이션 후 테스트 계획을 수행합니다.

마이그레이션 계획 중에 고안한 확인 작업을 수행하여 원래 로컬 구성에서와 마찬가지로 Panorama 푸시 구성에서도 방화벽이 효율적으로 작동하는지 확인합니다. 마이그레이션 후 테스트 계획 생성을 참조하세요.

 ©2024 Palo Alto Networks, Inc.

방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성 재사용

Panorama를 사용하여 관리하려는 HA 구성에 한 쌍의 방화벽이 있는 경우 구성이나 정책을 다시 만들 필요 없이 방화벽 HA 쌍의 로컬 구성을 Panorama로 가져올 수 있습니다. 이를 통해 기존 방화벽 구성을 재사용할 수 있습니다. 먼저 새 디바이스 그룹 및 템플릿을 만드는 데 사용되는 방화벽 구성을 Panorama로 가져옵니다. 로컬 방화벽 구성을 덮어쓰고 방화벽을 Panorama와 동기화하기 위해 방화벽에 대한 디바이스 그룹 및 템플릿의 특수 구성 푸시를 수행합니다.

방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성을 생성하려면 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성 푸시의 내용을 참조하십시오.

*Panorama*는 *PAN-OS 5.0* 이상의 버전을 실행하는 방화벽에서 구성을 가져올 수 있으며 해당 방화벽에 구성을 푸시할 수 있습니다. 예외는 *Panorama 6.1* 이상의 버전이 *PAN-OS 6.0.0 ~ 6.0.3*을 실행하는 방화벽에 구성을 푸시할 수 없다는 점입니다.

*Panorama*는 이미 관리되는 디바이스인 방화벽에서 구성을 가져올 수 있지만 디바이스 그룹이나 템플릿에 아직 할당되지 않은 경우에만 가능합니다.

STEP 1 | 마이그레이션을 계획합니다.

Panorama 관리로의 전환 계획의 체크리스트를 참조하십시오.

STEP 2 | HA 피어 간의 구성 동기화를 비활성화합니다.

HA 쌍의 두 방화벽에 대해 이 단계를 반복합니다.

1. 각 방화벽의 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 일반을 선택한 다음 설정 섹션을 편집합니다.
2. 구성 동기화 활성화를 선택 취소하고 확인을 클릭합니다.
3. 각 방화벽에서 구성 변경 사항을 커밋합니다.

STEP 3 | HA 방화벽을 Panorama 관리에 추가합니다.

Panorama 정책 및 개체, 디바이스 및 네트워크 템플릿이 활성화되어 있는지 확인합니다.

*Panorama*가 이미 이러한 방화벽에서 로그를 수신하는 경우 이 단계를 수행할 필요가 없습니다. 7단계를 진행합니다.

STEP 4 | Panorama 웹 인터페이스에 로그인하고 **Panorama** > 관리형 디바이스 > 요약을 선택한 후 각 방화벽의 디바이스 상태가 ###인지 확인합니다

	DEVICE NAME	VIRTUAL SYSTEM	MODEL	TAGS	SERIAL NUMBER	IP Address IPV4	I...	VARIABL...	TEMPLATE	DEVICE STATE	DEVICE CERTIFICATE	DEVICE CERTIFICATE EXPIRY DATE	HA STATUS
>	Alaap_LTD (2/2 Devices Connected): Shared > Alaap_LTD												
v	No Device Group Assigned (2/2 Devices Connected)												
	adept-vm-2		PA-VM		[redacted]	[redacted]		Edit		Connected			Passive
	adept-vm-1				[redacted]	[redacted]		Edit		Connected			Active

STEP 5 | 각 방화벽 구성을 Panorama로 가져옵니다.

©2024 Palo Alto Networks, Inc.

이 단계에서 디바이스 그룹 또는 템플릿 스택*(template stack)* 구성을 관리형 방화벽으로 푸시하지 마십시오. 이 단계에서 디바이스 그룹 및 템플릿 스택*(template stack)* 구성을 푸시하면 다음 단계에서 로컬 방화벽 *HA* 구성이 지워집니다.

나중에 방화벽 구성을 다시 가져오기로 결정한 경우 먼저 방화벽 디바이스 그룹과 템플릿이 구성원으로 있는 템플릿을 제거하십시오. 디바이스 그룹 및 템플릿 이름이 방화벽 호스트 이름과 동일한 경우 방화벽 구성을 다시 가져오기 전에 디바이스 그룹 및 템플릿을 삭제하거나 디바이스 그룹 이름 접두사 필드를 사용하여 다시 가져오기에 의해 생성된 디바이스 그룹 및 템플릿의 새 이름을 입력할 수 있습니다. 또한 방화벽은 디바이스 그룹 또는 템플릿에서 제거해도 로그가 손실되지 않습니다.

1. Panorama에서 **Panorama** > 설정 > 작업을 선택하고 **Panorama**로 디바이스 구성 가져오기를 클릭한 다음 디바이스를 선택합니다.

   *Panorama*는 기존 디바이스 그룹 또는 템플릿 스택*(template stack)*에 할당된 방화벽에서 구성을 가져올 수 없습니다.
2. (선택 사항) 템플릿 이름을 편집합니다. 기본값은 방화벽 이름입니다. 기존 템플릿 또는 템플릿 스택의 이름을 사용할 수 없습니다.
3. (선택 사항) 디바이스 그룹 이름을 편집합니다. Multi-VSYS 방화벽의 경우 각 디바이스 그룹에는 기본적으로 vsys 이름이 있으므로 각 디바이스 그룹 이름 접두사로 문자열을 추가하십시오. 그렇지 않으면 기본값은 방화벽 이름입니다. 기존 디바이스 그룹의 이름을 사용할 수 없습니다.

   불러온 디바이스의 공유 개체를 ***Panorama***의 공유 컨텍스트로 가져오기 확인란이 기본적으로 선택되어 있습니다. 즉, *Panorama*는 방화벽의 공유 위치에 속하는 가져오기 개체를 *Panorama*의 공유와 비교합니다. 불러온 개체가 방화벽의 공유 컨텍스트에 없으면 가져오는 각 디바이스 그룹에 적용됩니다. 확인란을 선택 취소하면 *Panorama* 복사본은 불러온 개체를 비교하지 않고 모든 공유 방화벽 개체를 공유 대신 가져오는 디바이스 그룹에 적용합니다. 이렇게 하면 중복 개체가 생성될 수 있으므로 대부분의 경우 확인란을 선택하는 것이 가장 좋습니다. 공유 또는 복제 개체를 *Panorama*로 가져올 때의 결과를 이해하려면 공유 설정 관리 방법 계획을 참조하십시오.
4. **Panorama**에 전념하십시오.
5. **Panorama** > 설정 > 작업을 선택하고 디바이스 구성 번들을 내보내거나 푸시합니다. 디바이스를 선택한 다음, 확인을 선택하고 구성을 푸시 및 커밋합니다.

   디바이스 그룹과 템플릿 스택*(template stack)*을 푸시하기 전에 두 방화벽에서 2단계의 *Enable Config Sync* 설정을 지워야 합니다.
6. 방화벽 HA 피어의 웹 인터페이스를 시작하고 이전 단계에서 푸시된 구성이 성공적으로 커밋되었는지 확인합니다. 그렇지 않은 경우 방화벽에서 로컬로 변경 사항을 커밋합니다.
7. 두 번째 방화벽에서 위의 1-6단계를 반복합니다. 이 프로세스는 각 방화벽마다 디바이스 그룹 및 템플릿 스택을 생성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | HA 방화벽 쌍을 동일한 디바이스 그룹 및 템플릿 스택(template stack)에 추가합니다.

(활성/활성 구성의 방화벽) 활성/활성 *HA* 구성의 방화벽에는 일반적으로 고유한 네트워크 구성이 필요하므로 *HA* 피어를 동일한 디바이스 그룹에 추가하지만 동일한 템플릿 스택에는 추가하지 않는 것이 좋습니다. 이것은 *HA* 피어에 대한 정책 관리를 단순화하는 동시에 네트워크 구성이 서로 독립적일 때 각 *HA* 피어의 네트워크 구성을 관리하는 운영 부담을 줄입니다. 예를 들어, 활성/활성 *HA* 구성의 방화벽은 호스트의 기본 게이트웨이로 사용되는 고유한 유동 *IP*와 같은 고유한 네트워크 구성이 필요한 경우가 많습니다.

궁극적으로 활성/활성 *HA* 구성의 방화벽을 동일한 디바이스 그룹 및 템플릿 스택에 추가할지 여부를 결정하는 것은 구성 계층 구조를 설계할 때 내려야 하는 설계 결정입니다.

1. **Panorama** > 디바이스 그룹을 선택한 다음 두 번째 방화벽의 디바이스 그룹을 선택하고 디바이스 그룹에서 두 번째 방화벽을 제거합니다.
2. 두 번째 방화벽을 제거한 디바이스 그룹을 선택한 다음 삭제합니다.
3. 첫 번째 방화벽에 대한 디바이스 그룹을 선택한 다음 두 번째 방화벽을 선택한 다음 확인을 클릭하고 **Panorama**에 커밋을 클릭하여 HA 피어와 동일한 디바이스 그룹에 추가합니다.
4. **Panorama** > 템플릿을 선택한 다음 두 번째 방화벽의 템플릿 스택을 선택하고 템플릿 스택에서 두 번째 방화벽을 제거합니다.
5. 두 번째 방화벽을 제거한 템플릿 스택을 선택한 다음 삭제합니다.
6. 첫 번째 방화벽에 대한 템플릿 스택을 선택한 다음 두 번째 방화벽을 추가하고 확인을 선택한 다음 **Panorama**에 커밋을 선택하여 HA 피어와 동일한 템플릿 스택에 추가합니다.
7. (선택 사항) 새로 마이그레이션된 방화벽과 연결된 템플릿에서 HA 설정을 제거합니다.

   *Panorama*에서 방화벽 *HA* 구성을 관리하거나 관리형 방화벽에서 로컬로 *HA* 설정을 구성할 수 있습니다.

   *Panorama*에서 방화벽 *HA* 설정을 관리하려면 이 단계를 건너뛰십시오.

   1. 디바이스 > 고가용성을 선택한 다음 HA 구성이 포함된 템플릿을 선택합니다.
   2. 모두 제거를 선택합니다.
   3. **Panorama**에 전념하십시오.
8. **Panorama** > 관리형 디바이스 > 요약을 선택한 다음 디바이스 그룹과 템플릿이 수동 방화벽에 대해 동기화되어 있는지 확인합니다. 수동 방화벽의 정책 규칙, 개체 및 네트워크 설정이 활성 방화벽과 일치하는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 디바이스 그룹 및 템플릿 스택(template stack) 구성 변경 사항을 관리형 방화벽으로 푸시합니다.

먼저 디바이스 그룹 및 템플릿 스택(template stack) 구성을 ### 또는 ###-## HA 피어에 먼저 푸시한 다음 ### 또는 ###-## HA 피어에 푸시해야 합니다.

로컬 방화벽 구성 업데이트를 제거하기 위해 *Panorama*에서 불러온 방화벽 구성 푸시 관리 방화벽에 대한 정책 규칙 사용을 모니터링할 때 새로 관리되는 방화벽에 푸시한 날짜를 반영하는 정책 규칙 생성 및 수정 날짜. 또한 각 정책 규칙에 대한 새로운 UUID(Universally Unique Identifier)가 생성됩니다.

1. ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 일시 중단합니다.
2. Panorama 관리 구성을 ## ### HA 방화벽으로 푸시합니다.
   1. Panorama 웹 인터페이스에 로그인합니다.
   2. 커밋 > 디바이스로 푸시를 선택한 다음 선택 사항을 편집합니다.
   3. 디바이스 후보 구성과 병합 및 디바이스 및 네트워크 템플릿 포함을 활성화(선택)합니다.

      (Panorama 관리형 HA 구성) 강제 템플릿 값을 활성화(선택)합니다.
   4. 디바이스 그룹 및 템플릿에서 일시 중단된 HA 방화벽을 선택합니다.
   5. 확인 및 푸시를 클릭합니다.
3. 일시 중단된 ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에서 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 작동시킵니다.
4. ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 일시 중단합니다.
5. 2단계를 반복하여 Panorama 관리 구성을 ## ### HA 피어에 푸시합니다.
6. 일시 중단된 ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 작동시킵니다.
7. Panorama 웹 인터페이스에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 디바이스 그룹과 템플릿이 HA 방화벽에 대해 동기화되어 있는지 확인합니다. 수동 방화벽의 정책 규칙, 개체 및 네트워크 설정이 활성 방화벽과 일치하는지 확인합니다.

STEP 8 | (로컬 방화벽 HA 구성만 해당) HA 피어 간의 구성 동기화를 활성화합니다.

동기화해야 하는 로컬 구성을 유지 관리하려는 경우 HA 쌍의 두 방화벽에 대해 이 단계를 반복합니다.

Panorama에서 방화벽 HA 구성을 관리하는 경우 이 단계를 건너뛰십시오. 이 설정은 기본적으로 활성화되어 있습니다.

1. 각 HA 피어의 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 일반을 선택한 후 설정 섹션을 편집합니다.
2. 구성 동기화 활성화를 선택한 다음 확인을 클릭합니다.
3. 각 방화벽에서 구성 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 새 구성 푸시

이 절차에서는 로컬 방화벽 구성을 *Panorama*에서 푸시된 구성으로 덮어씁니다.

방화벽 고가용성(HA) 쌍을 Panorama 관리로 마이그레이션하고 디바이스 그룹 및 템플릿 스택(template stack)을 사용하여 새로운 Panorama 관리형 구성을 생성합니다.

방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성을 재사용하려면 방화벽 HA 쌍을 Panorama 관리로 마이그레이션하고 기존 구성 재사용의 내용을 참조하십시오.

*Panorama*는 *PAN-OS 5.0* 이상의 버전을 실행하는 방화벽에서 구성을 가져올 수 있으며 해당 방화벽에 구성을 푸시할 수 있습니다. 예외는 *Panorama 6.1* 이상의 버전이 *PAN-OS 6.0.0 ~ 6.0.3*을 실행하는 방화벽에 구성을 푸시할 수 없다는 점입니다.

*Panorama*는 이미 관리되는 디바이스인 방화벽에서 구성을 가져올 수 있지만 디바이스 그룹이나 템플릿에 아직 할당되지 않은 경우에만 가능합니다.

STEP 1 | 마이그레이션을 계획합니다.

Panorama 관리로의 전환 계획의 체크리스트를 참조하십시오.

STEP 2 | HA 피어 간의 구성 동기화를 비활성화합니다.

HA 쌍의 두 방화벽에 대해 이 단계를 반복합니다.

1. 각 방화벽의 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 일반을 선택한 다음 설정 섹션을 편집합니다.
2. 구성 동기화 활성화를 선택 취소하고 확인을 클릭합니다.
3. 각 방화벽에서 구성 변경 사항을 커밋합니다.

STEP 3 | 방화벽을 관리되는 디바이스로 추가하십시오.

Panorama 관리에 방화벽을 추가하는 방법에 대한 자세한 내용은 관리형 디바이스로 방화벽 추가를 참조하십시오.

1. Panorama 웹 인터페이스에 로그인
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
   디바이스 등록 인증 키를 성공적으로 생성한 후 인증 키를 복사합니다.
3. **Panorama** > 관리되는 디바이스 > 요약을 선택하여 방화벽을 관리되는 디바이스로 추가합니다.
4. HA 쌍에 있는 각 방화벽의 일련번호를 입력하고 확인을 클릭합니다.

   여러 방화벽을 동시에 추가하려면 각 방화벽의 일련번호를 라인별로 입력합니다.
5. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 4 | 방화벽에서 Panorama로의 연결을 설정합니다.

HA 쌍의 두 방화벽에 대해 이 단계를 반복합니다.

1. 방화벽 웹 인터페이스에 로그인
2. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.

©2024 Palo Alto Networks, Inc.

3. **Panorama Servers** 필드에 Panorama 관리 서버의 IP 주소를 입력합니다.
4. 이전 단계에서 복사한 인증 키를 붙여넣습니다.
5. 확인 및 커밋을 클릭합니다.

STEP 5 | Panorama 웹 인터페이스에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 #### ##가 ## #인지 확인합니다.

STEP 6 | 디바이스 그룹 추가.

이 단계를 반복하여 방화벽 구성을 논리적으로 그룹화하는 데 필요한 만큼의 디바이스 그룹을 만듭니다. 디바이스 그룹은 디바이스 그룹 개체와 정책을 관리하는 데 필요합니다. 디바이스 그룹을 관리하는 방법에 대해 자세히 알아보십시오.

HA 피어를 동일한 디바이스 그룹에 추가해야 합니다.

STEP 7 | 템플릿 및 템플릿 스택(template stack)을 생성합니다.

템플릿 및 템플릿 스택(template stack)은 방화벽이 네트워크에서 작동할 수 있도록 방화벽 네트워크와 디바이스 설정을 구성하는 데 사용됩니다.

1. 템플릿 추가.

   이 단계를 반복하여 필요한 네트워킹 구성을 정의하는 데 필요한 만큼의 템플릿을 만듭니다.
2. 템플릿 스택(template stack) 구성.

   이 단계를 반복하여 정의된 네트워킹 구성을 빠르게 적용하는 데 필요한 만큼의 템플릿 스택(template stack)을 생성합니다. 템플릿 스택(template stack)을 생성할 때는 관련 템플릿과 관리형 방화벽을 할당합니다.

   HA 피어를 동일한 템플릿 스택(template stack)에 추가해야 합니다.

STEP 8 | 필요에 따라 디바이스 그룹, 템플릿 및 템플릿 스택(template stack)을 구성합니다.

STEP 9 | 디바이스 그룹 및 템플릿 스택(template stack) 구성 변경 사항을 관리형 방화벽으로 푸시합니다.

먼저 디바이스 그룹 및 템플릿 스택(template stack) 구성을 ### 또는 ###-## HA 피어에 먼저 푸시한 다음 ### 또는 ###-## HA 피어에 푸시해야 합니다.

1. ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 일시 중단합니다.
2. Panorama 관리 구성을 ## ### HA 방화벽으로 푸시합니다.
   1. Panorama 웹 인터페이스에 로그인합니다.
   2. 커밋 > 푸시 및 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
      - 디바이스 후보 구성과 병합 — 이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 Panorama의 구성 푸시와 병합합니다. 로컬 방화벽 구성은

 ©2024 Palo Alto Networks, Inc.

Panorama에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 병합되고 커밋됩니다.

Panorama 관리 구성과 별도로 로컬 방화벽 구성 변경 사항을 관리하고 커밋하는 경우 이 설정을 비활성화합니다.

- 템플릿 값 강제 적용 — 값이 충돌하는 경우 모든 로컬 방화벽 구성을 Panorama에서 푸시된 템플릿 스택(template stack) 구성의 값으로 덮어씁니다.

  이 설정은 기본적으로 활성화되어 있습니다. 이 설정을 활성화하면 충돌하는 방화벽 구성을 템플릿 또는 템플릿 스택(template stack)에 정의된 값으로 덮어씁니다. 이 설정을 활성화하기 전에 재정의된 값을 검토하여 중단이 발생하지 않도록 합니다.

3. 디바이스 그룹 및 템플릿에서 일시 중단된 HA 방화벽을 선택합니다.
4. 확인 및 푸시를 클릭합니다.

3. 일시 중단된 ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에서 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 작동시킵니다.
4. ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 일시 중단합니다.
5. 2단계를 반복하여 Panorama 관리 구성을 ## ### HA 피어에 푸시합니다.
6. 일시 중단된 ### 또는 ###-## HA 피어의 방화벽 웹 인터페이스에 로그인하고 디바이스 > 고가용성 > 작동 명령을 선택하여 고가용성을 위해 로컬 디바이스를 작동시킵니다.
7. Panorama 웹 인터페이스에서 **Panorama** > 관리되는 디바이스 > 요약을 선택하고 디바이스 그룹과 템플릿이 HA 방화벽에 대해 동기화되어 있는지 확인합니다. 수동 방화벽의 정책 규칙, 개체 및 네트워크 설정이 활성 방화벽과 일치하는지 확인합니다.

STEP 10 | **Panorama** > 관리되는 디바이스 > 요약을 선택하고 새로 추가된 방화벽에 대한 ## ##과 ### 상태가 ### #으로 되어 있는지 확인합니다.

방화벽 웹 인터페이스에서 구성 개체가 Panorama에서 푸시되었음을 나타내는 녹색 톱니바퀴가 표시되는지 확인합니다.

STEP 11 | 마이그레이션 후 테스트 계획을 수행합니다.

마이그레이션 계획 중에 고안한 확인 작업을 수행하여 원래 로컬 구성에서와 마찬가지로 Panorama 푸시 구성에서도 방화벽이 효율적으로 작동하는지 확인합니다. 마이그레이션 후 테스트 계획 생성을 참조하세요.

부분 방화벽 구성을 Panorama에 로드

방화벽의 일부 구성 설정이 다른 방화벽에 공통적인 경우 이러한 특정 설정을 Panorama에 로드한 다음 다른 모든 방화벽이나 특정 디바이스 그룹 및 템플릿의 방화벽에 푸시할 수 있습니다.

Panorama 관리 서버에 구성을 로드하려면 전체 커밋이 필요하며 운용 관리자가 수행해야 합니다. 구성 스냅샷 되돌리기 및 로드와 같은 특정 Panorama 작업을 수행할 때 전체 커밋이 필요하며 사용자 지정 관리자 역할 프로파일에는 지원되지 않습니다.

STEP 1 | Panorama로의 전환을 계획하십시오.

Panorama 관리로의 전환 계획의 체크리스트를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에서 방화벽과 동일한 이름을 가진 중복 설정을 관리하는 방법을 해결합니다.

부분 방화벽 구성을 로드하기 전에 Panorama와 해당 방화벽에 이미 중복 설정이 있을 수 있습니다. 방화벽 구성을 로드하면 다른 관리되는 방화벽의 설정과 중복되는 설정이 Panorama에 추가될 수도 있습니다.

*Panorama*에 방화벽에 있는 것과 동일한 이름을 가진 정책 규칙 또는 개체가 있는 경우 해당 방화벽에 디바이스 그룹 설정을 푸시하려고 하면 커밋 실패가 발생합니다. *Panorama*에 방화벽과 동일한 이름의 템플릿 설정이 있는 경우 템플릿을 푸시하면 템플릿 값이 방화벽 값보다 우선 적용됩니다.

1. Panorama에서 전역 찾기를 수행하여 중복 설정이 있는지 확인합니다.
2. Panorama를 사용하여 관리하려는 경우 방화벽에서 중복 설정을 삭제하거나 이름을 변경하거나 방화벽을 사용하여 관리하려는 경우 Panorama에서 중복 설정을 삭제하거나 이름을 변경합니다. 방화벽을 사용하여 디바이스 또는 네트워크 설정을 관리하는 경우 Panorama에서 중복 항목을 삭제하거나 이름을 바꾸는 대신 Panorama(6단계)에서 설정을 푸시한 다음 방화벽별 값을 사용하여 방화벽에서 템플릿 또는 템플릿 스택(template stack) 값 재정의 설정을 할 수도 있습니다.

STEP 3 | 전체 방화벽 구성을 로컬 컴퓨터로 내보냅니다.

1. 방화벽에서 디바이스 > 설정 > 작업을 선택합니다.
2. 명명된 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. 방화벽은 구성을 XML 파일로 내보냅니다.

STEP 4 | 방화벽 구성 스냅샷을 Panorama로 가져옵니다.

1. Panorama에서 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 컴퓨터로 내보낸 방화벽 구성 파일을 찾은 다음 확인을 클릭합니다.

이 옵션을 사용하여 방화벽 구성 파일을 불러온 후에는 *Panorama* 웹 인터페이스를 사용하여 이를 로드할 수 없습니다. 다음 단계에 설명된 대로 *XML API* 또는 *CLI*를 사용해야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 방화벽 구성의 원하는 부분을 Panorama에 로드합니다.

구성의 일부(예: 모든 애플리케이션 개체)를 지정하려면 다음을 식별해야 합니다.

- 소스 xpath - 로드 중인 방화벽 구성 파일의 XML 노드입니다.
- 대상 xpath - 로드 중인 Panorama 구성의 노드입니다.

XML API 또는 CLI를 사용하여 부분 구성을 식별하고 로드합니다.

1. 방화벽 XML API 또는 CLI를 사용하여 소스 xpath를 식별하십시오.

   예를 들어 방화벽의 vsys1에 있는 애플리케이션 개체에 대한 xpath는 다음과 같습니다.

   ```
   /config/devices/entry[@name='localhost.localdomain']/vsys/
   entry[@name='vsys1']/application
   ```

2. Panorama XML API 또는 CLI를 사용하여 대상 xpath를 식별합니다.

   예를 들어 애플리케이션 개체를 US-West라는 디바이스 그룹에 로드하려면 xpath는 다음과 같습니다.

   ```
   /config/devices/entry[@name='localhost.localdomain']/device-
   group/entry[@name='US-West']/application
   ```

3. Panorama CLI를 사용하여 구성을 로드하고 변경 사항을 커밋합니다.

   ```
   # load config partial mode [append|merge|replace]
    from-xpath <source-xpath> to-xpath <destination-xpath>
    from <filename> # commit
   ```

   예를 들어 다음을 입력하여 fw1-config.xml이라는 불러온 방화벽 구성의 vsys1에서 Panorama의 US-West라는 디바이스 그룹으로 애플리케이션 개체를 로드합니다.

   ```
   # load config partial mode merge from-xpath /config/
   devices/entry[@name='localhost.localdomain']/vsys/
   entry[@name='vsys1']/application to-xpath /config/
   devices/entry[@name='localhost.localdomain']/device-group/
   entry[@name='US-West']/application from fw1-config.xml
    # commit
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Panorama에서 방화벽으로 부분 구성을 푸시하여 중앙 집중식 관리로의 전환을 완료합니다.

1. 방화벽에서 Panorama와 동일한 이름을 가진 모든 규칙 또는 개체를 삭제합니다. 해당 방화벽의 디바이스 그룹에 Panorama에서 복제된 규칙 또는 개체가 있는 다른 방화벽이 있는 경우 해당 방화벽에서도 이 단계를 수행하십시오. 자세한 내용은 2단계를 참조하십시오.
2. Panorama에서 부분 구성을 방화벽으로 푸시합니다.
   1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
   2. 디바이스 그룹을 선택한 다음 불러온 방화벽 구성이 포함된 디바이스 그룹을 선택합니다.
   3. 디바이스 후보 구성과 병합, 디바이스 및 네트워크 템플릿 포함 및 템플릿 값 강제를 선택합니다.
   4. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
   5. 변경 사항을 커밋하고 푸시합니다.
3. 방화벽에 Panorama를 사용하여 관리하지 않을 디바이스 또는 네트워크 설정이 있는 경우 방화벽에서 템플릿 또는 템플릿 스택(template stack) 값 재정의을(를) 수행합니다.

STEP 7 | 마이그레이션 후 테스트 계획을 수행합니다.

마이그레이션 계획 중에 고안한 확인 작업을 수행하여 원래 로컬 구성에서와 마찬가지로 Panorama 푸시 구성에서도 방화벽이 효율적으로 작동하는지 확인합니다. 마이그레이션 후 테스트 계획 생성을 참조하세요.

관리되는 방화벽에서 Panorama 푸시 구성 현지화

Panorama™ 관리 서버에서 푸시된 템플릿 및 디바이스 그룹 구성을 다음으로 현지화할 수 있습니다.

- Panorama 관리에서 방화벽을 제거합니다.
- 방화벽 관리를 다른 Panorama로 마이그레이션합니다.
- Panorama에 액세스할 수 없는 긴급 상황의 경우 관리자가 관리되는 방화벽 구성을 로컬에서 수정할 수 있는지 확인하십시오.

STEP 1 | 운용 관리자 역할이 있는 관리자로 관리형 방화벽의 웹 인터페이스를 시작합니다. 브라우저 URL 필드에 IP 주소를 입력하거나 Panorama의 컨텍스트 드롭다운에서 방화벽을 선택하여 방화벽에 직접 액세스할 수 있습니다.

STEP 2 | (모범 사례) 디바이스 > 설정 > 작업 및 디바이스 상태 내보내기를 선택합니다.

관리되는 방화벽에서 알려진 작동 구성을 다시 로드해야 하는 경우 Panorama에서 푸시된 디바이스 그룹 및 템플릿 설정을 포함하여 방화벽 시스템 상태의 복사본을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | (능동/수동 HA 전용) 능동/수동 고가용성(HA) 구성에서 방화벽에 대한 구성 동기화를 비활성화합니다.

각 방화벽 HA 피어에서 이 단계를 반복합니다. 이는 로컬 커밋 실패를 초래하는 수동 HA 피어의 개체 복제를 방지하는 데 필요합니다.

1. HA 피어 중 하나의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 일반을 선택하고 HA 쌍 설정 설정을 편집합니다.
3. 설정 동기화 활성화를 비활성화(선택 취소)하고 확인을 클릭합니다.
4. 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 4 | 템플릿 구성을 비활성화하여 템플릿 및 템플릿 스택(template stack)을 사용하여 관리되는 방화벽의 네트워크 구성 개체를 관리하는 것을 중지합니다.

1. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
2. 디바이스 및 네트워크 템플릿 비활성화를 클릭합니다.
3. (선택 사항) 템플릿 구성 설정을 방화벽에 로컬로 저장하려면 비활성화하기 전에 디바이스 및 네트워크 템플릿 가져오기를 선택합니다. 이 옵션을 선택하지 않으면 PAN-OS는 방화벽에서 모든 Panorama 푸시 설정을 삭제합니다.
4. 계속하려면 확인을 두 번 클릭합니다.

STEP 5 | 디바이스 그룹 구성을 비활성화하여 디바이스 그룹을 사용하여 관리되는 방화벽의 정책 그룹 및 개체 구성을 관리하는 것을 중지합니다.

1. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
2. (선택 사항) 정책 규칙 및 개체 구성을 방화벽에 로컬로 저장하려면 비활성화하기 전에 **Panorama** 정책 개체 가져오기를 선택합니다. 이 옵션을 선택하지 않으면 PAN-OS는 방화벽에서 모든 Panorama 푸시 구성을 삭제합니다.
3. 계속하려면 확인을 클릭하세요.



다음 단계가 성공적으로 완료될 때까지 모든 커밋이 실패하므로 아직 관리형 방화벽에서 구성 변경 사항을 커밋하려고 시도하지 마십시오.

STEP 6 | 디바이스 > 설정 > 작업 및 이름이 지정된 구성 스냅샷 저장을 선택합니다.

STEP 7 | 명명된 구성 스냅샷을 로드하고 선택한 명명된 구성에 대해 규칙 **UUID** 재생성을 활성화(선택)하여 새 정책 규칙 UUID를 생성합니다.

이 단계는 관리되는 방화벽에서 Panorama 푸시 정책 규칙을 성공적으로 현지화하는 데 필요합니다.

STEP 8 | 확인을 클릭하여 명명된 구성 스냅샷을 로드합니다.

STEP 9 | 명명된 구성 스냅샷 로드를 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 10 | (액티브/패시브 HA만) 액티브/패시브 하이 HA 구성에서 방화벽에 대한 구성 동기화를 활성화합니다.

방화벽 HA 피어마다 이 단계를 반복합니다.

1. HA 피어 중 하나의 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 고가용성 > 일반을 선택하고 HA 쌍 설정 설정을 편집합니다.
3. 구성 동기화 사용을 활성화(선택)하고 확인을 클릭합니다.
4. 커밋을 선택하고 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 디바이스 모니터링

방화벽을 추가하고 정책 규칙을 구성한 후 상태를 모니터링하여 방화벽이 정상적인 매개변수 내에서 작동하는지 확인할 수 있습니다. 정책 규칙의 경우 규칙 트래픽 일치를 모니터링하여 트래픽 시행 요구 사항과 일치하는 규칙을 식별합니다.

- 디바이스 상태 모니터링
- 정책 규칙 사용 모니터링

디바이스 상태 모니터링

관리 방화벽의 상태 정보를 모니터링하여 네트워크 보안에 영향을 미치기 전에 하드웨어 문제를 식별하고 해결합니다. Panorama™ 및 관리 방화벽은 모두 PAN-OS® 8.1 이상의 버전을 실행해야 하지만 방화벽은 요약 세션, 로깅, 리소스 및 환경 성능을 모니터링하기 위해 디바이스 그룹 또는 템플릿 스택(template stack)의 일부일 필요가 없습니다. Panorama는 관리 방화벽의 지난 90일 상태 모니터링 통계를 저장하므로 방화벽을 선택하면 세션, 환경, 인터페이스, 로깅, 리소스 및 고가용성 성능에 대한 시간 추세 그래프와 테이블을 볼 수 있습니다.

Panorama는 7일 평균 및 표준 편차를 사용하여 각 메트릭의 기준 성능을 계산하여 특정 방화벽의 정상 작동 범위를 결정합니다. 관리형 디바이스 상태 데이터의 상위 수준 개요를 볼 때 표시되는 값입니다. 디바이스, CPS, 세션, 데이터 플레인, 관리 플레인 또는 로깅 속도 상태 메트릭 값을 클릭하여 스냅샷을 볼 수 있습니다. 기준선, 24시간, 7일 및 15일 평균을 포함하여 해당 특정 지표에 대한 자세한 상태 데이터를 보여줍니다. 상태 메트릭 스냅샷을 보면 기준선을 추적하고 시간별 추세 성능을 비교할 수 있을 뿐만 아니라, 어떤 방화벽에 편차가 있는 메트릭이 있는지 확인하고 성능 관련 문제가 네트워크에 영향을 미치기 전에 격리할 수 있습니다. Panorama는 지표가 정상 작동 범위 밖에 있음을 식별하면 지표를 표시하고 일탈 디바이스 탭을 일탈 방화벽으로 채웁니다.

상태 모니터링 데이터는 Panorama에 저장되며 방화벽이 제거된 경우에도 보존됩니다. Panorama 관리에서 방화벽이 제거되면 상태 모니터링 데이터가 더 이상 표시되지 않지만 90일 동안 보존됩니다. 90일이 지나면 제거된 방화벽의 모든 상태 모니터링 데이터가 Panorama에서 제거됩니다. 방화벽이 Panorama 관리에 다시 추가되면 방화벽이 제거되었을 때의 최신 상태 모니터링 데이터가 표시됩니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | **Panorama** > 관리형 디바이스 > 상태를 선택하여 관리형 방화벽의 상태를 모니터링합니다.

모든 디바이스 보기에서 관리되는 모든 방화벽 및 모니터링되는 상태 메트릭 목록을 볼 수 있습니다. 개별 방화벽을 선택하여 모니터링되는 메트릭의 시간 추세 그래프 및 테이블과 함께 자세한 디바이스 보

 ©2024 Palo Alto Networks, Inc.

기를 봅니다. 디바이스, CPS, 세션, 데이터 플레인, 관리 플레인 또는 로깅 속도 상태 메트릭 값을 클릭하여 스냅샷을 보고 해당 특정 상태 메트릭에 대한 자세한 추가 정보를 볼 수 있습니다.

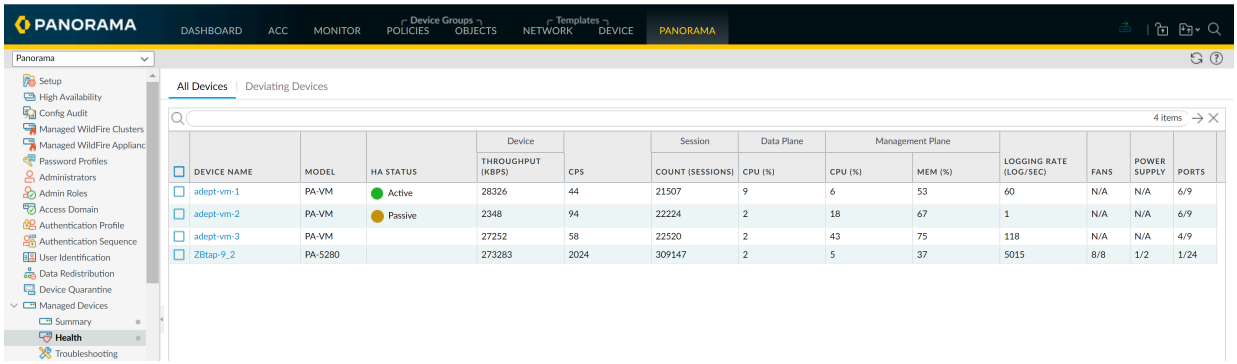


그림 **11:** 관리 방화벽 상태 모니터링

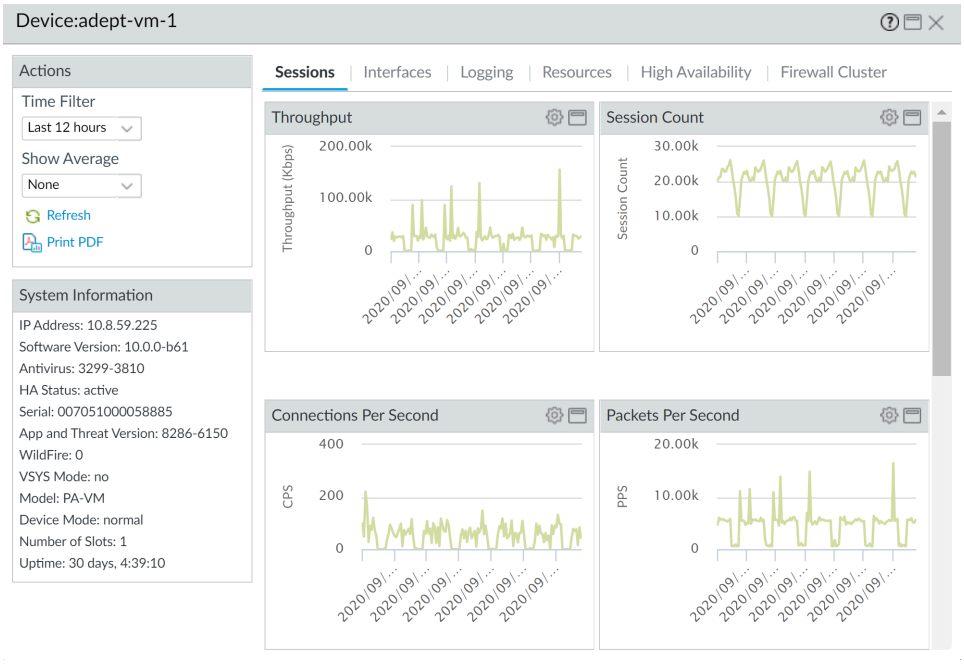


그림 **12:** 상세 디바이스 보기

 ©2024 Palo Alto Networks, Inc.

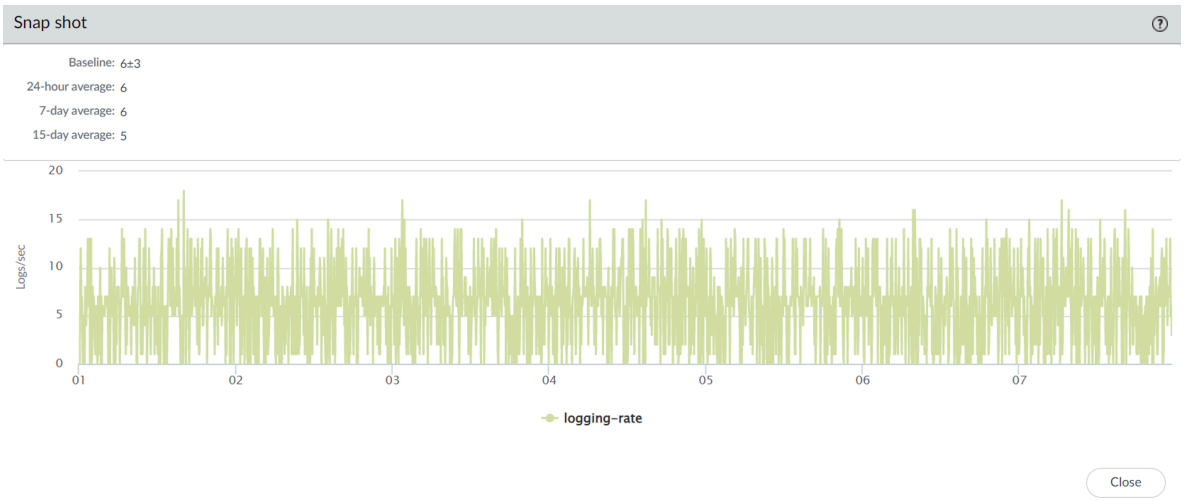
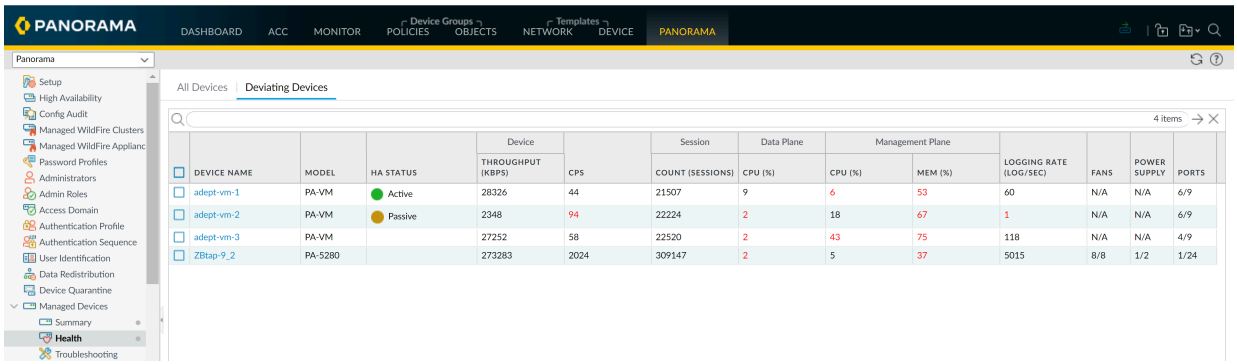


그림 **13:** 메트릭 스냅샷

STEP 3 | 계산된 기준을 벗어난 상태 메트릭이 있는 방화벽을 보려면 편차 디바이스를 선택합니다.

Panorama는 계산된 기준에서 벗어나는 메트릭을 보고하는 모든 방화벽을 나열하고 이탈 메트릭을 빨간색으로 표시합니다.



정책 규칙 사용 모니터링

정책이 변경되면 Panorama의 추적 규칙 사용은 정책 구현이 계속해서 시행 요구 사항과 일치하는지 평가하는 데 도움이 됩니다. 이러한 가시성을 통해 사용하지 않는 규칙을 식별 및 제거하여 보안 위험을 줄이고 정책 규칙 기반을 체계적으로 유지할 수 있습니다. 또한 규칙 사용 추적을 통해 새 규칙 추가 및 규칙 변경을 빠르게 검증하고 작업 및 문제 해결 작업에 대한 규칙 사용을 모니터링할 수 있습니다. Panorama에서는 정책을 푸시한 디바이스 그룹에서 방화벽의 규칙 사용을 확인하여, 디바이스 그룹의 모든 방화벽에서 방화벽 전체에 걸친 총 적중 수만 모니터링할 수 있는 대신 트래픽이 일치하는 방화벽이 모두 있는지, 일부 또는 전혀 없는지 확인할 수 있습니다. 사용자 지정 가능한 시간 프레임 내에서 생성 날짜 및 수정 날짜와 같은 규칙 사용 데이터를 사용하여 규칙을 빠르게 필터링할 수 있습니다. 표시된 규칙 사용 정보는 재부팅, 데이터플레인 다시 시작 및 업그레이드 후에도 지속됩니다.

Panorama에서는 PAN-OS 8.1 이상의 버전을 실행하고 있고 정책 규칙 적중 횟수가 활성화(기본값)되어 있으며 디바이스 그룹을 사용하여 정책 규칙을 정의하고 푸시한 관리 방화벽에 대한 규칙 사용 세부 정보를 볼 수 있습니다. Panorama는 방화벽에 로컬로 구성된 정책 규칙에 대한 규칙 사용 세부 정보를 검색할 수 없으므로 로컬로 구성된 규칙에 대한 규칙 사용 정보를 보려면 방화벽에 로그인해야 합니다.

 ©2024 Palo Alto Networks, Inc.

정책 규칙 베이스를 필터링한 후 관리자는 정책 최적화 프로그램에서 직접 정책 규칙을 삭제, 비활성화, 활성화 및 태그를 지정하는 조치를 취할 수 있습니다. 예를 들어 사용하지 않는 규칙을 필터링한 다음 검토를 위해 태그를 지정하여 규칙 베이스에서 안전하게 삭제할 수 있는지 또는 유지할 수 있는지 결정할 수 있습니다. 관리자가 정책 최적화 프로그램에서 직접 조치를 취할 수 있도록 함으로써 규칙 수명 주기 관리를 단순화하고 방화벽이 과도하게 프로비저닝되지 않도록 하는 데 필요한 관리 오버헤드를 줄일 수 있습니다.

정책 규칙 사용 데이터는 정책 최적화 프로그램을 사용하여 먼저 마이그레이션하거나 정리할 규칙의 우선 순위를 지정할 때 유용할 수도 있습니다.

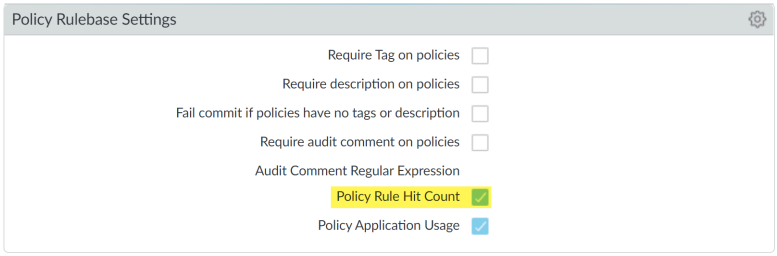
다른 Panorama 모델로 전환할 때 정책 규칙 사용 데이터는 보존되지 않습니다. 즉, 새 *Panorama* 모델로 성공적으로 마이그레이션한 후에는 이전 *Panorama*의 모든 기존 정책 규칙 사용 데이터가 더 이상 표시되지 않습니다. 마이그레이션이 성공하면 *Panorama*는 마이그레이션 완료 날짜를 기준으로 정책 규칙 사용 데이터를 추적하기 시작합니다. 예를 들어, ## 날짜에는 마이그레이션이 완료된 날짜가 표시됩니다.

모든 공유 규칙 또는 특정 디바이스 그룹에 대한 규칙 사용을 보려면 다음을 따릅니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 정책 규칙 적중 횟수가 활성화되어 있는지 확인합니다.

1. 정책 규칙 베이스 설정(**Panorama** > 설정 > 관리.)
2. 정책 규칙 적중 횟수가 활성화되어 있는지 확인합니다.



STEP 3 | 정책 을 선택하여 > ***<policy rule>***규칙을 봅니다.

STEP 4 | 디바이스 그룹 컨텍스트를 공유로 변경하거나 보려는 특정 디바이스 그룹으로 변경합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 규칙이 사용되고 있는지 확인합니다(규칙 사용). 정책 규칙 사용 상태는 다음 중 하나입니다.

방화벽은 규칙 사용을 결정하기 위해 Panorama에 대해 정책 규칙 적중 횟수가 활성화된 PAN-OS 8.1 이상의 버전을 실행해야 합니다.

- 사용됨 - 정책 규칙을 푸시한 디바이스 그룹의 모든 방화벽에 정책 규칙과 일치하는 트래픽이 있는 경우.
- 부분적으로 사용됨 - 정책 규칙을 푸시한 디바이스 그룹의 일부 방화벽에 정책 규칙과 일치하는 트래픽이 있는 경우.
- 미사용 - 정책 규칙을 푸시한 디바이스 그룹의 방화벽에 정책 규칙과 일치하는 트래픽이 없는 경우.
- **Em-dash(—)** - 정책 규칙을 푸시한 디바이스 그룹에 방화벽이 없는 경우 Panorama에서 규칙 사용을 결정하기 위해 정책 규칙 적중 횟수를 활성화하거나 사용할 수 있습니다.
- 수정됨 - 정책 규칙이 마지막으로 수정된 날짜 및 시간입니다.
- 생성됨 - 정책 규칙이 생성된 날짜 및 시간입니다.

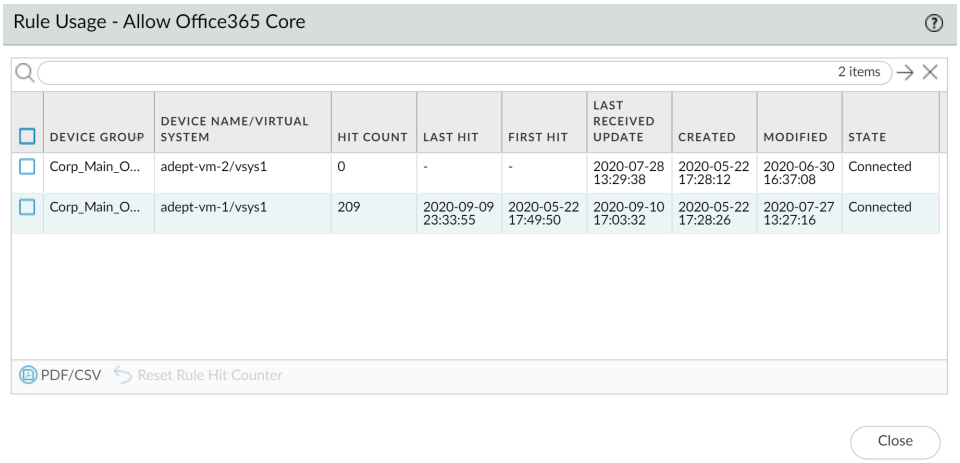


*Panorama*가 *PAN-OS 8.1*을 실행할 때 규칙이 생성되었고 정책 규칙 적중 횟수 설정이 활성화된 경우 *PAN-OS 9.0* 이상 버전으로 업그레이드할 때 첫 번째 적중 날짜 및 시간이 생성 날짜 및 시간으로 사용됩니다. 정책 규칙 적중 횟수 설정이 비활성화되었을 때 *PAN-OS 8.1*에서 규칙이 생성되었거나 *Panorama*가 *PAN-OS 8.0* 또는 이전 버전을 실행할 때 규칙이 생성된 경우 규칙의 생성 날짜는 *Panorama*를 *PAN-OS 9.0* 이상 버전으로 성공적으로 업그레이드한 날짜 및 시간이 됩니다.

Rule Usage		DAYS WITH NO NEW APPS	MODIFIED	CREATED
RULE USAGE	APPS SEEN			
Used	6	150	2020-06-24 10:34:...	2020-04-09 11:34:03
Unused	0	-	2020-06-24 10:34:...	2020-04-16 11:42:46
Used	11	57	2020-06-24 10:34:...	2020-04-16 11:42:46
Partially Used	3	111	2020-06-24 10:34:...	2020-05-22 17:26:44
Unused	0	-	2020-06-24 10:34:...	2020-05-22 22:45:53

©2024 Palo Alto Networks, Inc.

STEP 6 | 규칙 사용 상태를 클릭하여 규칙을 사용하는 방화벽 목록과 각 방화벽에서 해당 규칙과 일치하는 트래픽의 적중 횟수 데이터를 봅니다.



STEP 7 | (선택 사항) 디바이스 그룹의 개별 방화벽에 대한 정책 규칙 적중 횟수 데이터를 봅니다.

1. 미리보기 규칙을 클릭합니다.
2. 디바이스 컨텍스트에서 정책 규칙 사용 데이터를 보려는 방화벽을 선택합니다.

STEP 8 | 정책을 선택한 다음 정책 최적화 대화 상자에서 규칙 사용 필터를 확인합니다.

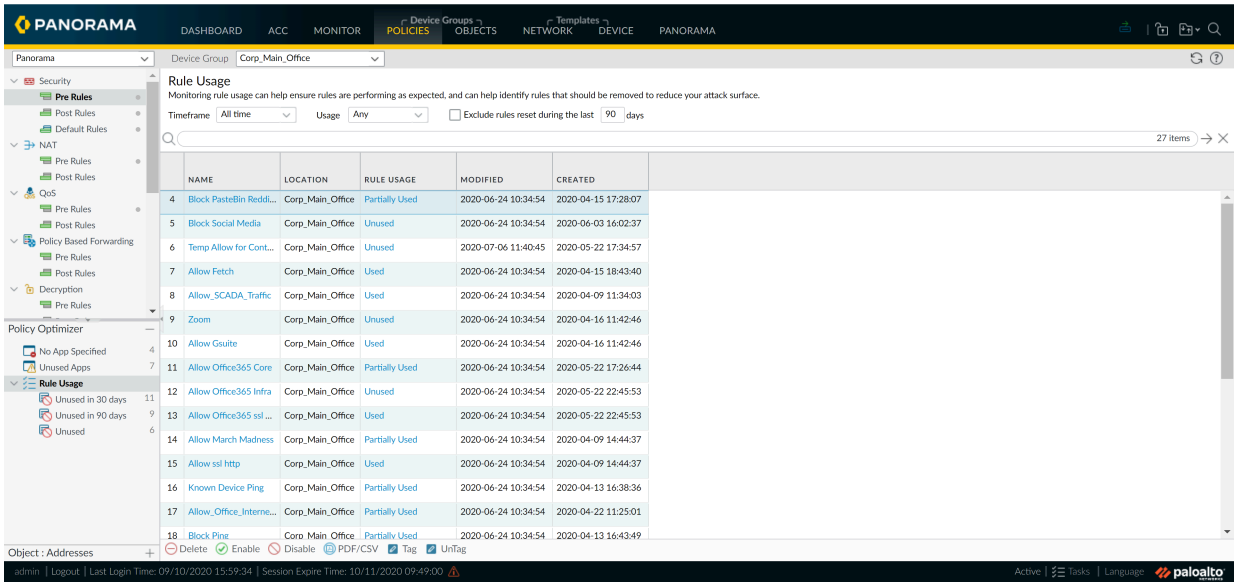
 ©2024 Palo Alto Networks, Inc.

STEP 9 | 선택한 규칙 베이스에서 규칙을 필터링합니다.

Panorama에서 방화벽으로 푸시된 규칙에 대한 규칙 사용을 필터링할 수 있습니다. Panorama는 방화벽에 로컬로 구성된 규칙에 대한 규칙 사용을 필터링할 수 없습니다.

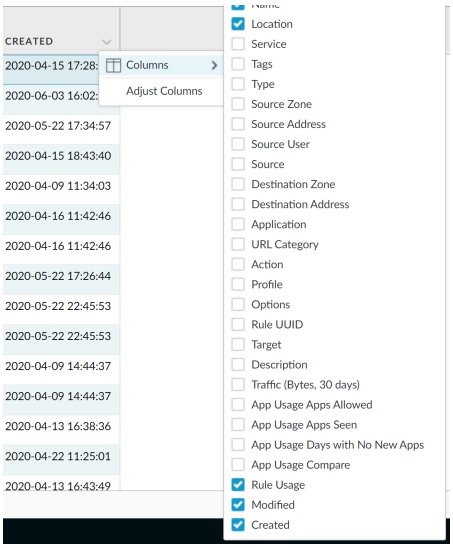
규칙 사용 필터를 사용하여 지정된 기간 내의 규칙 사용을 평가합니다. 예를 들어, 지난 *30*일 이내에 사용하지 않은 규칙에 대해 선택한 규칙 베이스를 필터링합니다. 작성된 날짜 및 수정한 날짜와 같은 다른 규칙 속성을 사용하여 규칙 사용을 평가할 수도 있습니다. 이를 통해 검토할 올바른 규칙 세트를 필터링할 수 있습니다. 이 데이터를 사용하여 규칙 수명 주기를 관리하고 네트워크 공격 면적을 줄이기 위해 규칙을 제거해야 하는지의 여부를 결정할 수 있습니다.

1. 필터링할 기간을 선택하거나 사용자 지정 기간을 지정합니다.
2. 필터링할 규칙 사용을 선택합니다.
3. (선택 사항) 규칙에 대한 규칙 사용 데이터를 재설정한 경우 지난 ***<number of days>***일 동안 재설정된 규칙 제외를 확인하고 규칙이 재설정된 이후 지정한 일수를 기준으로 규칙을 제외할 시기를 결정합니다. 지정된 일 수 전에 재설정된 규칙만 필터링된 결과에 포함됩니다.

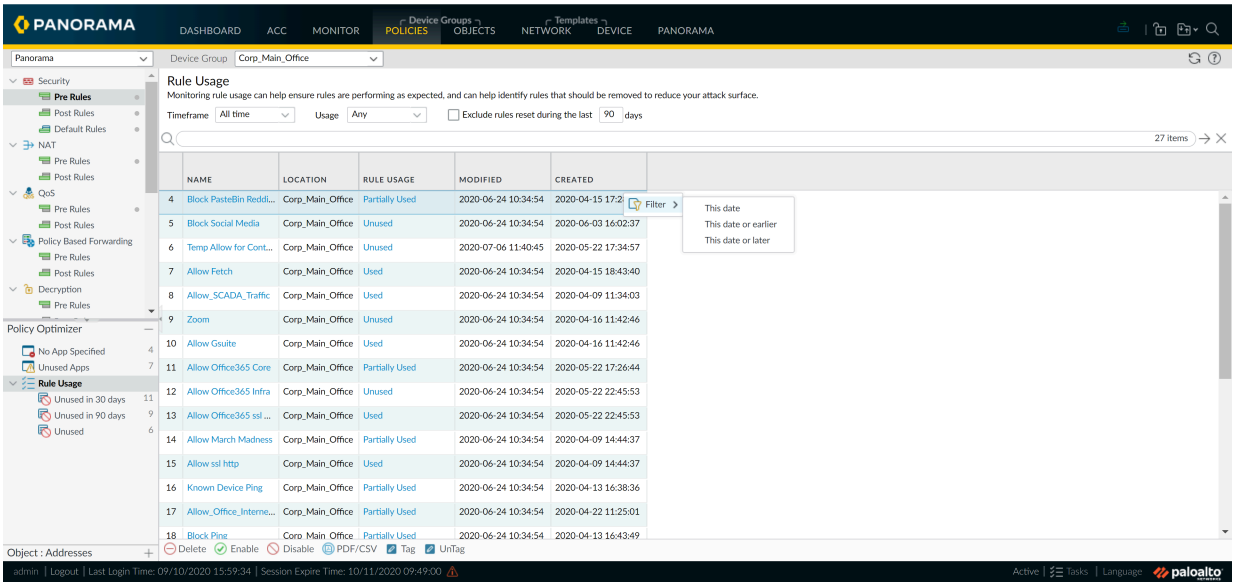


4. (선택 사항) 규칙 사용 이외의 추가 규칙 데이터를 기반으로 검색 필터를 지정합니다.
   1. 열 머리글 위로 마우스를 가져간 다음 드롭다운에서 열을 선택합니다.
   2. 필터링하거나 표시할 열을 추가합니다.

©2024 Palo Alto Networks, Inc.



3. 필터링할 열 데이터 위로 마우스를 가져간 다음 드롭다운에서 필터를 선택합니다. 날짜가 포함된 데이터의 경우 해당 날짜, 해당 날짜 이전 또는 해당 날짜 이후를 사용하여 필터링할지의 여부를 선택합니다.
4. 필터 적용(→)을 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 10 | 하나 이상의 사용하지 않는 정책 규칙에 대해 조치를 취하십시오.

1. 사용하지 않는 정책 규칙을 하나 이상 선택하십시오.
2. 다음 작업 중 하나를 수행합니다.
   - 삭제 - 선택한 정책 규칙을 하나 이상 삭제합니다.
   - 활성화 - 비활성화된 경우 선택한 정책 규칙을 하나 이상 활성화합니다.
   - 비활성화 - 선택한 정책 규칙을 하나 이상 비활성화합니다.
   - 태그 - 하나 이상의 선택한 정책 규칙에 하나 이상의 그룹 태그를 적용합니다. 정책 규칙에 태그를 지정하려면 그룹 태그가 이미 존재해야 합니다.
   - 태그 해제 - 하나 이상의 선택한 정책 규칙에서 하나 이상의 그룹 태그를 제거합니다.
3. 커밋을 선택한 다음 변경 사항을 커밋 및 푸시합니다.

©2024 Palo Alto Networks, Inc.

사용 사례: Panorama를 사용하여 방화벽 구성

고가용성 구성에서 Panorama를 사용하여 네트워크에서 12개의 방화벽을 관리하려고 한다고 가정해 보겠습니다. 6개의 지사에 6개의 방화벽, 2개의 데이터 센터 각각에 고가용성 구성의 한 쌍의 방화벽, 2개의 지역 본사 각각에 1개의 방화벽이 있습니다.

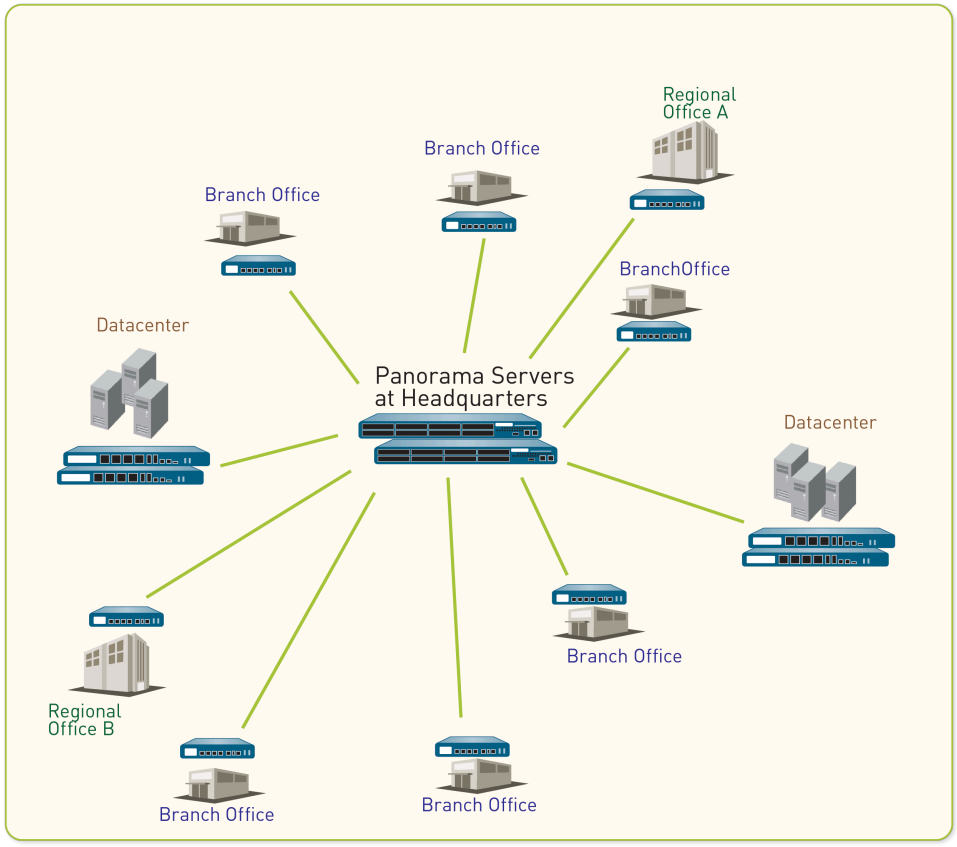


그림 **14:** 방화벽 배포 예

중앙 관리 전략을 만드는 첫 번째 단계는 Panorama에서 구성을 효율적으로 푸시하기 위해 방화벽을 디바이스 그룹 및 템플릿으로 그룹화하는 방법을 결정하는 것입니다. 방화벽의 비즈니스 기능, 지리적 위치 또는 관리 도메인을 기준으로 그룹화할 수 있습니다. 이 예에서는 Panorama를 사용하여 방화벽을 관리하기 위해 2개의 디바이스 그룹과 3개의 템플릿을 생성합니다.

- 이 사용 사례의 디바이스 그룹
- 이 사용 사례의 템플릿
- 중앙 집중식 구성 및 정책 설정

이 사용 사례의 디바이스 그룹

사용 사례: Panorama를 사용하여 방화벽 구성에서는 방화벽이 수행할 기능에 따라 두 개의 디바이스 그룹을 정의해야 합니다.

©2024 Palo Alto Networks, Inc.

- 지사 및 지역 본사에서 보안 게이트웨이 역할을 하는 방화벽을 그룹화하기 위한 DG_BranchAndRegional. 기능이 유사한 방화벽에는 유사한 정책 규칙 기반이 필요하기 때문에 지점 방화벽과 지역 사무실 방화벽을 동일한 디바이스 그룹에 배치했습니다.
- 데이터 센터에서 서버를 보호하는 방화벽을 그룹화하기 위한 DG_DataCenter.

그런 다음 두 디바이스 그룹에서 공유 정책 규칙을 관리할 수 있을 뿐만 아니라 지역 사무소 및 지점 그룹에 대해 고유한 디바이스 그룹 규칙을 관리할 수 있습니다. 그런 다음 유연성을 높이기 위해 지역 또는 지점의 로컬 관리자는 해당 사무실에 필요한 애플리케이션 및 서비스에 액세스하기 위한 특정 소스, 대상 및 서비스 흐름과 일치하는 로컬 규칙을 만들 수 있습니다. 이 예에서는 보안 규칙에 대해 다음 계층을 생성합니다. 다른 모든 규칙 베이스에 대해 유사한 접근 방식을 사용할 수 있습니다.

Device Groups	DG_BranchAndRegional		DG_DataCenter
Rules	**Regional**	**Branch**	**Datacenter**
Shared pre-rule	Allow DNS and SNMP services.		
	Acceptable use policy that denies access to specified URL categories and peer-to-peer traffic that is of risk level 3, 4, and 5.		
Device Group pre-rule	Allow Facebook to all users in the marketing group in the regional offices only.		Allow access to the Amazon cloud application for the specified hosts/servers in the datacenter.
Local rules on a device	None		
Device Group post-rule	None		
Shared post-rule	To enable logging for all Internet-bound traffic on your network, create a rule that allows or denies all traffic from the trust zone to the untrust zone.		

그림 **15:** 보안 규칙 계층

이 사용 사례의 템플릿

템플릿에 대한 방화벽을 그룹화할 때 네트워킹 구성의 차이점을 고려해야 합니다. 예를 들어, 인터페이스 구성이 동일하지 않은 경우(인터페이스 유형이 다르거나 사용된 인터페이스가 번호 지정 체계 및 링크 용량에서 유사하지 않거나 영역 대 인터페이스 매핑이 다른 경우) 방화벽은 별도의 템플릿에 있어야 합니다. 또한 방화벽이 지리적으로 분산되어 있기 때문에 네트워크 리소스에 액세스하도록 방화벽을 구성하는 방식이 다를 수 있습니다. 예를 들어 액세스하는 DNS 서버, syslog 서버 및 게이트웨이가 다를 수 있습니다. 따라서 최적의 기본 구성을 허용하려면 사용 사례: Panorama를 사용하여 방화벽 구성에서 방화벽을 다음과 같이 별도의 템플릿에 배치해야 합니다.

- 지사 방화벽용 T_Branch
- T_지역 사무실 방화벽을 위한 지역

 ©2024 Palo Alto Networks, Inc.

- 데이터 센터 방화벽을 위한 T_DataCenter

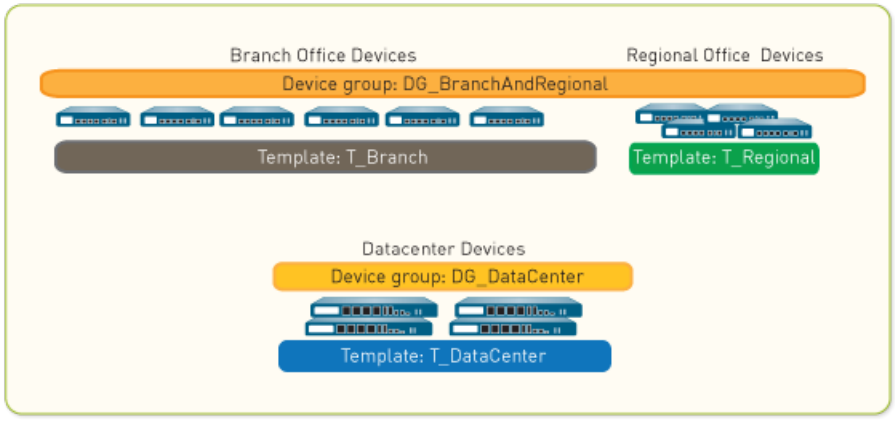


그림 **16:** 디바이스 그룹 예

활성/활성 *HA* 구성으로 방화벽을 배포하려는 경우 *HA* 쌍의 각 방화벽을 별도의 템플릿에 할당합니다. 이렇게 하면 각 피어에 대해 별도의 네트워킹 구성을 유연하게 설정할 수 있습니다. 예를 들어, 각 피어에 대해 별도의 템플릿에서 네트워킹 구성을 관리하여 각각이 서로 다른 노스바운드 및 사우스바운드 라우터에 연결할 수 있고 서로 다른 *OSPF* 또는 *BGP* 피어링 구성을 가질 수 있습니다.

중앙 집중식 구성 및 정책 설정

사용 사례: Panorama를 사용하여 방화벽 구성에서 방화벽을 중앙에서 배포하고 관리하려면 다음 작업을 수행해야 합니다.

- 관리 방화벽 추가 및 업데이트 배포
- 템플릿을 사용하여 기본 구성 관리
- 디바이스 그룹을 사용하여 정책 규칙 푸시
- 규칙 미리보기 및 변경 사항 커밋

관리 방화벽 추가 및 업데이트 배포

사용 사례: Panorama를 사용하여 방화벽 구성의 첫 번째 작업은 방화벽을 관리 디바이스로 추가하고 해당 방화벽에 콘텐츠 업데이트 및 PAN-OS 소프트웨어 업데이트를 배포하는 것입니다.

STEP 1 | Panorama가 관리할 각 방화벽에 대한 내용은 관리되는 디바이스로 방화벽 추가입니다.

이 예에서는 12개의 방화벽을 추가합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 콘텐츠 업데이트를 방화벽에 배포합니다. Threat Prevention 구독을 구입한 경우 콘텐츠 및 바이러스 백신 데이터베이스를 사용할 수 있습니다. 먼저 애플리케이션 또는 애플리케이션 및 위협 데이터베이스를 설치한 다음 바이러스 백신을 설치합니다.

*Panorama*에서 수행된 모든 작업의 상태 또는 진행 상황을 검토하려면 Panorama 작업 관리자 사용을(를) 참조하십시오.

1. **Panorama** > 디바이스 배포 > 동적 업데이트를 선택합니다.
2. 지금 확인을 클릭하여 최신 업데이트를 확인합니다. 작업 열의 값이 다운로드이면 업데이트가 있음을 나타냅니다.
3. 다운로드를 클릭합니다. 다운로드가 완료되면 작업 열의 값이 설치로 변경됩니다.
4. 작업 열에서 설치를 클릭합니다. 필터 또는 사용자 정의 태그를 사용하여 이 업데이트를 설치할 관리되는 방화벽을 선택합니다.
5. 확인을 클릭한 다음 각 방화벽에 대한 콘텐츠 업데이트의 상태, 진행률 및 결과를 모니터링합니다. 결과 열에는 설치의 성공 또는 실패가 표시됩니다.

STEP 3 | 방화벽에 소프트웨어 업데이트를 배포합니다.

1. **Panorama** > 디바이스 배포 > 소프트웨어를 선택합니다.
2. 지금 확인을 클릭하여 최신 업데이트를 확인합니다. 작업 열의 값이 다운로드이면 업데이트가 있음을 나타냅니다.
3. 각 하드웨어 모델에 필요한 버전을 찾고 다운로드를 클릭합니다. 다운로드가 완료되면 작업 열의 값이 설치로 변경됩니다.
4. 작업 열에서 PAN-OS 버전을 확인하면 업그레이드에 필요한 모든 중간 소프트웨어 및 콘텐츠 버전을 볼 수 있습니다.

   PAN-OS 버전을 확인하려면 Panorama가 인터넷에 연결되어 있어야 합니다.
5. 작업 열에서 설치 링크를 클릭합니다. 필터 또는 사용자 정의 태그를 사용하여 이 버전을 설치할 관리되는 방화벽을 선택합니다.
6. (선택 사항) 설치 후 디바이스 재부팅의 체크박스를 활성화합니다.
7. 확인을 클릭합니다. 결과 열에는 설치 성공 또는 실패가 표시됩니다.

템플릿을 사용하여 기본 구성 관리

사용 사례의 두 번째 작업: Panorama를 사용하여 방화벽 구성은 기본 구성을 방화벽으로 푸시하는 데 필요한 템플릿을 만드는 것입니다.

STEP 1 | 사용할 각 템플릿에 대해 템플릿을 추가하고 각각에 적절한 방화벽을 할당합니다.

이 예에서는 T_Branch, T_Regional 및 T_DataCenter라는 템플릿을 생성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | DNS 서버, NTP 서버, syslog 서버 및 로그인 배너를 정의합니다. 각 템플릿에 대해 이 단계를 반복합니다.

1. 디바이스 탭의 드롭다운에서 템플릿을 선택합니다.
2. DNS 및 NTP 서버를 정의합니다.
   1. **Device** > **Setup** > **Services** > **Global**을 선택한 다음 서비스를 편집합니다.
   2. 서비스 탭에서 기본 **DNS** 서버의 IP 주소를 입력합니다.

      둘 이상의 가상 시스템(*vsys*)이 있는 방화벽의 경우 각 *vsys*에 대해 템플릿(***Device*** > ***Server Profiles*** > ***DNS***)에 DNS 서버 프로파일을 추가합니다.
   3. **NTP** 탭에서 기본 **NTP** 서버의 IP 주소를 입력합니다.
   4. 확인을 클릭하여 변경 사항을 저장합니다.
3. 로그인 배너 추가: 디바이스 > 설정 > 관리를 선택한 다음 일반 설정을 편집하고 로그인 배너에 대한 텍스트를 입력하고 확인을 클릭합니다.
4. Syslog 서버 프로파일을 구성합니다(디바이스 > 서버 프로파일 > **Syslog**).

STEP 3 | 관리되는 방화벽의 관리 인터페이스에 대한 HTTPS, SSH 및 SNMP 액세스를 활성화합니다. 각 템플릿에 대해 이 단계를 반복합니다.

1. 디바이스 탭의 드롭다운에서 템플릿을 선택합니다.
2. 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 편집합니다.
3. 서비스에서 **HTTPS**, **SSH** 및 **SNMP** 체크박스을 선택한 다음 확인을 클릭합니다.

STEP 4 | 데이터 센터 템플릿(T_DataCenter)에서 방화벽에 대한 영역 보호 프로파일을 생성합니다.

1. 네트워크 탭을 선택한 다음 템플릿 드롭다운에서 T_DataCenter를 선택합니다.
2. 네트워크 프로파일 > 영역 보호를 선택한 다음 추가를 클릭합니다.
3. 이 예의 경우 SYN 플러드에 대한 보호 활성화 - 플러드 보호 탭에서 **SYN** 체크박스를 선택한 다음 작업을 **SYN** 쿠키로 설정하고 경고 패킷/초를 **100**으로 설정하고 패킷/초 활성화를 **1000**으로 설정한 다음 최대 패킷/초를 **10000**으로 설정합니다.
4. 이 예의 경우 경고 활성화 - 정찰 보호 탭에서 **TCP** 포트 스캔, 호스트 스윕 및 **UDP** 포트 스캔에 대해 활성화 체크박스를 선택합니다. 조치 값이 경고(기본값)로 설정되었는지 확인합니다.
5. 확인을 클릭하여 영역 보호 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 데이터 센터 템플릿(T_DataCenter)에서 인터페이스 및 영역 설정을 구성한 다음 방금 생성한 Zone Protection 프로파일을 연결합니다.

이 단계를 수행하기 전에 방화벽에서 로컬로 인터페이스를 구성해야 합니다. 최소한 각 인터페이스에 대해 인터페이스 유형을 정의하고 가상 라우터에 할당하고(필요한 경우) 보안 영역을 연결해야 합니다.

1. 네트워크 탭을 선택한 다음 템플릿 드롭다운에서 T_DataCenter를 선택합니다.
2. 네트워크 > 인터페이스를 선택한 다음 인터페이스 열에서 인터페이스 이름을 클릭합니다.
3. 드롭다운에서 인터페이스 유형을 선택합니다.
4. 가상 라우터 드롭다운에서 새 가상 라우터를 클릭합니다. 라우터를 정의할 때 이름이 방화벽에 정의된 것과 일치하는지 확인합니다.
5. 보안 영역 드롭다운에서 새 영역을 클릭합니다. 영역을 정의할 때 이름이 방화벽에 정의된 것과 일치하는지 확인합니다.
6. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
7. 네트워크 > 영역을 선택한 다음 방금 생성한 영역을 선택합니다. 올바른 인터페이스가 존에 연결되어 있는지 확인합니다.
8. 영역 보호 프로파일 드롭다운에서 생성한 프로파일을 선택한 다음 확인을 클릭합니다.

STEP 6 | 템플릿 변경 사항을 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 템플릿을 선택한 다음 변경한 템플릿에 할당된 방화벽을 선택합니다.
3. Panorama 구성 및 템플릿에 대한 변경 사항을 커밋하고 푸시합니다.

디바이스 그룹을 사용하여 정책 규칙 푸시

사용 사례의 세 번째 작업: Panorama를 사용하여 방화벽 구성은 디바이스 그룹을 생성하여 방화벽에 대한 정책 규칙을 관리하는 것입니다.

STEP 1 | 디바이스 그룹을 생성하고 각 디바이스 그룹에 적절한 방화벽을 할당합니다. 디바이스 그룹 추가를 참조하십시오.

이 예에서는 DG_BranchAndRegional 및 DG_DataCenter라는 디바이스 그룹을 생성합니다.

DG_BranchAndRegional 디바이스 그룹을 구성할 때 마스터 방화벽을 할당해야 합니다. 이것은 정책 평가를 위해 사용자 및 그룹 매핑 정보를 수집하는 디바이스 그룹의 유일한 방화벽입니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | DNS 및 SNMP 서비스를 허용하는 공유 사전 규칙을 생성합니다.

1. DNS 및 SNMP 서비스에 대한 공유 애플리케이션 그룹을 생성합니다.
   1. 개체 > 애플리케이션 그룹을 선택한 다음 추가를 클릭합니다.
   2. 이름을 입력하고 공유 체크박스을 선택하여 공유 애플리케이션 그룹 개체를 생성합니다.
   3. 추가를 클릭하고 **DNS**를 입력한 다음 목록에서 **dns**를 선택합니다. SNMP에 대해 반복하고 **snmp**, **snmp-trap**을 선택합니다.
   4. 확인을 클릭하여 애플리케이션 그룹을 생성합니다.
2. 공유 규칙을 생성합니다.
   1. 정책 탭을 선택한 다음 디바이스 그룹 드롭다운에서 공유를 선택합니다.
   2. 보안 > 사전 규칙 규칙 베이스를 선택하십시오.
   3. 추가를 클릭하고 보안 규칙의 이름을 입력합니다.
   4. 규칙에 대한 소스 및 대상 탭에서 추가를 클릭하고 트래픽에 대한 소스 영역 및 대상 영역을 입력합니다.
   5. 애플리케이션 탭에서 추가를 클릭하고 방금 생성한 애플리케이션 그룹 개체의 이름을 입력한 다음 드롭다운에서 선택합니다.
   6. 작업 탭에서 작업을 허용으로 설정하고 확인을 클릭합니다.

STEP 3 | 모든 사무실에 대한 회사의 사용 제한 정책을 정의합니다. 이 예에서는 일부 URL 카테고리에 대한 액세스를 제한하고 위험 수준 3, 4 또는 5인 P2P 트래픽에 대한 액세스를 거부하는 공유 규칙을 생성합니다.

1. 정책 탭을 선택한 다음 디바이스 그룹 드롭다운에서 공유를 선택합니다.
2. 보안 > 사전 규칙을 선택한 다음 추가를 클릭합니다.
3. 일반 탭에서 보안 규칙의 이름을 입력합니다.
4. 소스 및 대상 탭에서 추가를 클릭하고 트래픽 소스 영역 및 대상 영역에 대하여 **any**를 선택합니다.
5. 애플리케이션 탭에서 애플리케이션 필터를 정의합니다.
   1. 추가를 클릭하고 드롭다운 바닥글에서 새 애플리케이션 필터를 클릭합니다.
   2. 이름을 입력하고 공유 체크박스을 선택합니다.
   3. 위험 열에서 수준 **3**, **4** 및 **5**를 선택합니다.
   4. 기술 열에서 피어 투 피어를 선택합니다.
   5. 확인을 클릭하여 새 필터를 저장합니다.
6. 서비스/**URL** 카테고리 탭의 URL 카테고리 섹션에서 추가를 클릭하고 차단할 카테고리(예: 스트리밍 미디어, 날짜 및 온라인 개인 스토리지)를 선택합니다.
7. 기본 URL 필터링 프로파일을 연결할 수도 있습니다. 작업 탭의 프로파일 설정 섹션에서 프로파일 유형 옵션 프로파일을 선택한 다음 **URL** 필터링 옵션 기본값을 선택합니다.
8. 확인을 클릭하여 보안 사전 규칙을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 지역 사무소의 마케팅 그룹에 속한 모든 사용자에게만 Facebook을 허용합니다.

사용자 및 그룹을 기반으로 보안 규칙을 활성화하려면 다음과 같은 전제 조건 작업이 필요합니다.

- 방화벽에서 사용자 ID를 설정합니다.
- 식별하려는 사용자가 포함된 각 영역에 대해 User-ID를 활성화합니다.
- DG_BranchAndRegional 디바이스 그룹에 대한 마스터 방화벽을 정의합니다(1단계 참조).

1. 정책 탭을 선택한 다음 디바이스 그룹 드롭다운에서 DG_BranchAndRegional을 선택합니다.
2. 보안 > 사전 규칙 규칙 베이스를 선택하십시오.
3. 추가를 클릭하고 보안 규칙의 이름을 입력합니다.
4. 소스 탭에서 마케팅 그룹 사용자가 포함된 소스 영역을 추가합니다.
5. 대상 탭에서 대상 영역을 추가합니다.
6. 사용자 탭에서 마케팅 사용자 그룹을 소스 사용자 목록에 추가합니다.
7. 애플리케이션 탭에서 추가를 클릭하고 **Facebook**을 입력한 다음 드롭다운에서 선택합니다.
8. 작업 탭에서 작업을 허용으로 설정합니다.
9. 대상 탭에서 지역 사무실 방화벽을 선택한 다음 확인을 클릭합니다.

STEP 5 | 데이터 센터의 지정된 호스트/서버에 대해 Amazon 클라우드 애플리케이션에 대한 액세스를 허용합니다.

1. Amazon 클라우드 애플리케이션에 액세스해야 하는 데이터 센터의 서버/호스트에 대한 주소 객체를 생성합니다.
   1. 개체 > 주소를 선택한 다음 디바이스 그룹 드롭다운에서 DG_DataCenter를 선택합니다.
   2. 추가를 클릭하고 주소 개체의 이름을 입력합니다.
   3. 유형을 선택한 다음 IP 주소 및 넷마스크(**IP** 넷마스크), IP 주소 범위(**IP** 범위) 또는 **FQDN**을 지정합니다.
   4. 확인을 클릭하여 개체를 저장합니다.
2. Amazon 클라우드 애플리케이션에 대한 액세스를 허용하는 보안 규칙을 생성합니다.
   1. 정책 > 보안 > 사전 규칙을 선택한 다음 디바이스 그룹 드롭다운에서 DG_DataCenter를 선택합니다.
   2. 추가를 클릭하고 보안 규칙의 이름을 입력합니다.
   3. 소스 탭, 데이터 센터에 대한 소스 영역 추가 및 방금 정의한 주소 개체(소스 주소) 추가를 선택합니다.
   4. 대상 탭을 선택한 다음 대상 영역을 추가합니다.
   5. 애플리케이션 탭을 선택한 다음 추가를 클릭하고 **amazon**을 입력하고 목록에서 Amazon 애플리케이션을 선택합니다.
   6. 작업 탭을 선택한 다음 작업을 허용으로 설정합니다.
   7. 규칙을 저장하려면 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 네트워크의 모든 인터넷 바인딩 트래픽에 대한 로깅을 활성화하려면 신뢰 영역을 신뢰하지 않는 영역과 일치시키는 규칙을 생성합니다.

1. 정책 탭을 선택한 다음 디바이스 그룹 드롭다운에서 공유를 선택합니다.
2. 보안 > 사전 규칙 규칙 베이스를 선택하십시오.
3. 추가를 클릭하고 보안 규칙의 이름을 입력합니다.
4. 규칙의 원본 및 대상 탭에서 **trust_zone**을 원본 영역으로 추가하고 **untrust_zone**을 대상 영역으로 추가합니다.
5. 작업 탭에서 작업을 거부로 설정하고 로그 설정을 세션 종료 시 기록으로 설정한 다음 확인을 클릭합니다.

규칙 미리보기 및 변경 사항 커밋

사용 사례: Panorama를 사용하여 방화벽 구성의 마지막 작업은 규칙을 검토하고 Panorama, 디바이스 그룹 및 템플릿에 대한 변경 사항을 커밋하는 것입니다.

STEP 1 | 규칙을 미리 봅니다.

이 미리보기를 사용하면 특정 규칙 베이스에 대해 규칙이 계층화되는 방식을 시각적으로 평가할 수 있습니다.

1. 정책 및 미리 보기 규칙을 선택합니다.
2. 규칙 베이스, 디바이스 그룹 및 디바이스를 선택합니다.
3. 완료되면 미리보기 대화 상자를 닫습니다.

STEP 2 | 구성 변경 사항을 커밋하고 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 디바이스 그룹을 선택한 다음 추가한 디바이스 그룹을 선택한 다음 디바이스 및 네트워크 템플릿 포함을 선택합니다.
3. (선택 사항) Panorama의 구성 변경과 별도로 로컬 방화벽 구성 변경을 관리하는 경우디바이스 후보 구성과 병합을 비활성화합니다.

   이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 Panorama의 구성 푸시와 병합합니다. 로컬 방화벽 구성은 Panorama에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 로컬 방화벽 구성이 병합되고 커밋됩니다.
4. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
5. 변경 사항을 커밋하고 푸시합니다.

STEP 3 | Panorama가 템플릿 및 정책 구성을 적용했는지 확인합니다.

1. Panorama 헤더에서 컨텍스트를 방화벽으로 설정하여 웹 인터페이스에 액세스합니다.
2. 템플릿 및 정책 구성을 검토하여 변경 사항이 있는지 확인하십시오.

 ©2024 Palo Alto Networks, Inc.

로그 수집 관리

모든 Palo Alto Networks 방화벽은 방화벽 활동에 대한 감사 추적을 제공하는 로그를 생성할 수 있습니다. 중앙 집중식 로깅 및 보고의 경우 방화벽에서 생성된 로그를 Panorama™ 관리 서버 또는 로그 수집기를 포함하는 온프레미스 인프라로 포워딩하거나 로그를 클라우드 기반 Strata Logging Service로 보내야 합니다. 선택적으로 로그를 외부 로깅 대상(예: syslog 서버)으로 포워딩하도록 Panorama를 구성할 수 있습니다.

레거시 모드에서 Panorama 가상 어플라이언스에 로그를 포워딩하는 경우 로깅을 활성화하기 위해 추가 작업을 수행할 필요가 없습니다. 로그 수집기에 로그를 포워딩하는 경우 관리 수집기로 구성하고 수집기 그룹에 할당해야 합니다. 관리형 수집기는 M-시리즈 어플라이언스 또는 Panorama 모드의 Panorama 가상 어플라이언스에 로컬일 수 있습니다. 또한 로그 수집기 모드의 M-시리즈 어플라이언스 또는 Panorama 가상 어플라이언스는 전용 로그 수집기가 될 수 있습니다. 관리되는 수집기 유형 중 하나 또는 둘 다를 배포할지의 여부를 결정하려면 로컬 및 분산 로그 수집을 참조하세요.

Panorama가 로컬에서 생성하는 시스템 및 구성 로그를 관리하려면 Panorama 모니터링을 참조하십시오.

- 관리형 수집기 구성
- 관리형 수집기 상태 모니터링
- 전용 로그 수집기에 대한 인증 구성
- 수집기 그룹 관리
- Panorama에 대한 로그 포워딩 구성
- 외부 대상에 대한 Syslog 포워딩 구성
- 로그를 Strata Logging Service로 포워딩
- Panorama로 로그 포워딩 확인
- 로그 포워딩 및 버퍼링 기본값 수정
- Panorama에서 외부 대상으로 로그 포워딩 구성
- 로그 수집 배포

관리형 수집기 구성

Panorama 관리 서버가 Log Collector를 관리할 수 있도록 하려면 이를 관리형 수집기로 추가해야 합니다. 로그 수집기는 상호 인증을 위해 사용자 지정 인증서를 구성하는 경우를 포함하여 공용 또는 개인 IPv4 또는 IPv6 주소만 사용하는 통신을 지원합니다.

두 가지 유형의 관리형 수집기를 추가할 수 있습니다.

- 전용 로그 수집기 - 새 M-700, M-600, M-500, M-300 또는 M-200 기기 또는 Panorama 가상 기기를 로그 수집기로 설정하여 기존 M-시리즈 기기 또는 Panorama 가상 기기를 Panorama 모드에서 로그 수집기 모드로 전환하려면, M-시리즈 어플라이언스를 로그 수집기로 설정해야 합니다. Panorama 모드에서 로그 수집기 모드로 전환하면 Panorama 모드의 M-시리즈 어플라이언스에 사전 정의된 로컬 로그 수집기가 제거됩니다.
- 로컬 로그 수집기 - 로그 수집기는 M-700, M-600, M-500, M-300, M-200 기기 또는 Panorama 모드의 Panorama 가상 기기에서 로컬로 실행할 수 있습니다. M-Series 어플라이언스에서 Log Collector는 사전 정의됩니다. 가상 어플라이언스에서 Log Collector를 추가해야 합니다. Panorama 관리 서버에 고가용성(HA) 구성이 있는 경우 각 HA 피어는 로컬 로그 수집기를 가질 수 있습니다. 그러나 기본 Panorama와 관련하여 보조 Panorama의 로그 수집기는 로컬이 아닌 원격입니다. 따라서 보조 Panorama에서 로그 수집기를 사용하려면 기본 Panorama에 수동으로 추가해야 합니다(자세한 내용은 로컬 로그 수집기로 Panorama M-시리즈 어플라이언스 배포 또는 로컬 로그 수집기로 Panorama 가상 어플라이언스 배포 참조). 로컬 로그 수집기를 삭제한 경우 나중에 다시 추가할 수 있습니다. 다음 단계에서는 로컬 로그 수집기를 추가하는 방법을 설명합니다.

Panorama 가상 어플라이언스가 레거시 모드인 경우 Panorama 모드로 전환하여 Log Collector를 생성해야 합니다. 자세한 내용은 로컬 로그 수집기로 Panorama 가상 어플라이언스 설정을 참조하십시오.

디바이스 등록 인증 키는 처음 연결할 때 Panorama 관리 서버와 관리형 수집기를 안전하게 인증하고 연결하는 데 사용됩니다. 디바이스 등록 인증 키를 구성하려면 키 수명과 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 횟수를 지정하십시오. 또한 인증 키가 유효한 하나 이상의 Log Collector 일련번호를 지정할 수 있습니다.

인증 키는 키 수명이 만료된 후 90일이 지나면 만료됩니다. 90일이 지나면 유효성을 유지하기 위해 인증 키를 다시 인증하라는 메시지가 표시됩니다. 재인증을 하지 않으면 인증키가 무효가 됩니다. Log Collector가 Panorama 생성 인증 키를 사용할 때마다 시스템 로그가 생성됩니다. Log Collector는 모든 후속 통신에 사용되는 디바이스 인증서를 포워딩할 때 인증 키를 사용하여 Panorama를 인증합니다.



최선의 방법은 전용 로그 수집기를 관리하는지의 여부에 관계없이 *Panorama* 관리 서버에 로컬 로그 수집기 및 수집기 그룹을 유지하는 것입니다.



(Panorama 평가 전용*)* 로컬 로그 수집기로 *Panorama* 가상 어플라이언스를 평가하는 경우, Panorama에서 외부 대상으로 로그 포워딩 구성을*(*를*)* 수행하여, 평가 기간 동안 생성된 로그를 보존합니다.

로컬 로그 수집기를 사용하여 평가 Panorama 인스턴스를 프로덕션 Panorama 인스턴스로 변환할 때 로컬 로그 수집기에 저장된 로그는 보존할 수 없습니다.

 ©2024 Palo Alto Networks, Inc.

PAN-OS 10.1 릴리즈를 실행하는 전용 로그 수집기의 경우 *PAN-OS 11.1*을 실행하는 *Panorama*는 *PAN-OS 10.1.3* 이상 릴리즈만 실행하는 전용 로그 수집기 온보딩을 지원합니다. *Panorama*가 *PAN-OS 11.0*을 실행 중인 경우 *PAN-OS 10.1.2* 또는 이전 *PAN-OS 10.1* 릴리스를 실행하는 전용 로그 수집기를 *Panorama* 관리에 추가할 수 없습니다.

*Panorama*는 다음 릴리스를 실행하는 온보딩 전용 로그 수집기를 지원합니다.

- ***PAN-OS 10.2*** 이상 릴리스를 실행하는 ***Panorama*** - *PAN-OS 10.1.3* 이상 릴리스를 실행하는 전용 로그 수집기 및 *PAN-OS 10.0* 또는 이전 *PAN-OS* 릴리스를 실행하는 전용 로그 수집기.

PAN-OS 10.2 이상 릴리스로 업그레이드해도 *Panorama*에서 이미 관리하는 전용 로그 수집기에 영향을 미치지 않습니다.

Panorama 관리에 전용 로그 수집기를 추가하는 데 문제가 발생한 경우 Panorama에 대해 관리되는 디바이스 연결을 복구해야 할 수 있습니다.

STEP 1 | 로그 수집기의 일련번호를 기록합니다.

로그 수집기를 관리 수집기로 추가할 때 일련번호가 필요합니다.

1. Panorama 웹 인터페이스에 액세스합니다.
2. 대시보드를 선택한 다음 일반 정보 섹션에 일련번호를 기록합니다.

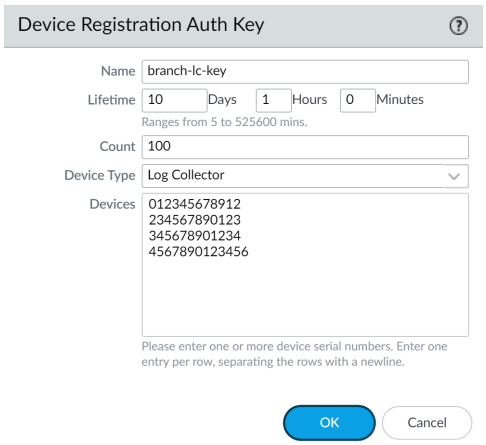
STEP 2 | Panorama 웹 인터페이스에 로그인.

STEP 3 | 기기 등록 인증 키를 생성합니다.

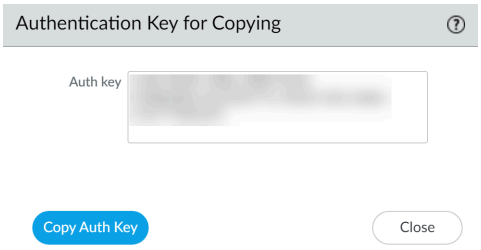
1. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
2. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 기간에 대한 키 수명을 지정합니다.
   - 개수 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 로그 수집기를 인증하는 데만 사용되도록 지정합니다.

     모두를 선택하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩하는 디바이스 등록 인증 키를 사용할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 로그 수집기를 지정할 하나 이상의 디바이스 일련번호를 입력합니다.
3. 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.



4. 인증 키를 복사하고 닫습니다.



STEP 4 | (전용 로그 수집기만 해당) 로그 수집기에 디바이스 등록 인증 키를 추가합니다.

전용 로그 수집기에만 디바이스 등록 인증 키를 추가합니다. Panorama 모드의 Panorama는 자체 로컬 로그 수집기를 인증할 필요가 없습니다.

1. 로그 수집기 CLI에 로그인합니다.
2. 디바이스 등록 인증 키를 추가합니다.

```
admin> ## # ## <auth-key> ##
```



STEP 5 | 로그 수집기를 관리 수집기로 추가합니다.

1. Panorama 웹 인터페이스에서**Panorama** > 관리형 수집기를 선택하고 새 로그 수집기를 추가합니다.
2. 일반 설정에서 로그 수집기에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.
4. 커밋 > **Panorama**에 커밋을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | (선택 사항) 로그 수집기 관리자 인증을 구성합니다.

*Palo Alto Networks*는 관리되는 수집기에 대한 권한 부여 목록을 구성하는 경우인증에 대한 수퍼유저 권한이 있는 로컬 관리자를 한 명 이상 추가할 것을 권장합니다.

가져온 *Panorama* 관리자를 추가한 경우 수퍼유저 권한이 있는 로컬 관리자를 한 명 이상 추가해야 합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 이름을 클릭하여 Log Collector를 편집합니다.
2. 로그 수집기 관리자 암호를 구성합니다.
   1. 비밀번호 모드를 선택하세요.
   2. 암호 모드를 선택한 경우 일반 텍스트 암호 및 암호 확인을 입력합니다. 암호 해시 모드를 선택한 경우 최대 63자의 해시된 암호 문자열을 입력합니다.
3. 관리자 로그인 보안 요구 사항을 구성합니다.

   실패한 시도를 *0* 이외의 값으로 설정했지만 잠금 시간을 *0*으로 두면 다른 관리자가 잠긴 관리자의 잠금을 수동으로 해제할 때까지 관리자가 무기한 잠깁니다. 다른 관리자가 생성되지 않은 경우 *Panorama*에서 실패한 시도 및 잠금 시간 설정을 재구성하고 구성 변경 사항을 로그 수집기로 푸시해야 합니다. 관리자가 잠기지 않도록 하려면 실패한 시도 및 잠금 시간 모두에 대해 기본값 *0*을 사용하십시오.

   1. 로그인 실패 횟수 값을 입력합니다. 범위는 기본값 **0**에서 최대 **10** 사이이며 값 **0**은 무제한 로그인 시도를 지정합니다.
   2. 기본값 **0**에서 최대 **60**분 사이의 잠금 시간 값을 입력합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 7 | 로깅 디스크를 활성화합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 이름을 클릭하여 Log Collector를 편집합니다.

   Log Collector 이름은 Panorama 관리 서버의 호스트 이름과 동일한 값을 갖습니다.
2. 디스크를 선택하고 각 디스크 쌍을 추가합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.
4. 커밋 > **Panorama**에 커밋을 선택합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | (선택 사항) 배포에서 Panorama와 관리되는 디바이스 간의 인증에 사용자 지정 인증서를 사용하는 경우 사용자 지정 클라이언트 디바이스 인증서를 배포합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택한 다음 드롭다운에서 인증서 프로파일을 선택하거나 새 인증서 프로파일을 클릭하여 생성합니다.
2. **Panorama** > **Managed Collectors**를 선택하고 새 로그 수집기를 추가하거나 기존 수집기를 선택합니다. 통신을 선택합니다.
3. 유형 드롭다운에서 디바이스 인증서 유형을 선택합니다.
   - 로컬 디바이스 인증서를 사용하는 경우 해당 드롭다운에서 인증서 및 인증서 프로파일을 선택합니다.
   - SCEP를 디바이스 인증서로 사용하는 경우 해당 드롭다운에서 **SCEP** 프로파일 및 인증서 프로파일을 선택합니다.
4. 확인을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | (선택 사항) 로그 수집기에서 보안 서버 통신을 구성합니다. 자세한 내용은 사용자 지정 인증서를 사용하여 인증 설정을 참조하십시오.

1. **Panorama** > 관리형 수집기를 선택하고 추가를 클릭합니다. 통신을 선택합니다.
2. 사용자 지정 인증서만 확인란이 선택되어 있지 않은지 확인합니다. 이를 통해 사용자 지정 인증서로 마이그레이션하는 동안 모든 디바이스를 계속 관리할 수 있습니다.

   Custom Certificate Only 확인란을 선택하면 *Log Collector*가 인증되지 않고 사전 정의된 인증서를 사용하여 디바이스에서 로그를 수신할 수 없습니다.
3. SSL/TLS 서비스 프로파일 드롭다운에서 **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 로그 수집기와 로그를 보내는 디바이스 간의 모든 SSL 연결에 적용됩니다.
4. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
5. 서버가 관리되는 디바이스의 일련번호에 대해 클라이언트를 확인하도록 하려면 일련번호를 기반으로 클라이언트 인증을 선택합니다. 클라이언트 인증서에는 일련번호를 기반으로 권한을 부여하는 CN으로 특수 키워드 $UDID가 설정되어 있어야 합니다.
6. 연결 끊기 대기 시간(분)에 Panorama가 관리 디바이스와의 연결을 끊고 다시 설정하기 전에 기다려야 하는 시간(분)을 입력합니다. 이 필드는 기본적으로 비어 있으며 범위는 0~44,640분입니다.

   연결 해제 대기 시간은 새 구성을 커밋할 때까지 카운트다운을 시작하지 않습니다.
7. (선택 사항) 권한 부여 목록을 구성합니다.
   1. 권한 부여 목록을 추가합니다.
   2. 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 선택한 유형의 식별자를 지정합니다.
   4. 확인을 클릭합니다.
   5. 권한 부여 목록을 적용하려면 로그 수집기가 권한 부여 목록을 확인하도록 설정하십시오.
8. 확인을 클릭합니다.
9. 커밋 > **Panorama**에 커밋을 선택합니다.

STEP 10 | 변경 사항을 확인하십시오.

1. **Panorama** > 관리형 수집기 페이지에 추가한 로그 수집기가 나열되는지 확인합니다. 연결됨 열에는 로그 수집기가 Panorama에 연결되었음을 나타내는 확인 표시가 표시됩니다. 페이지에 업데이트된 연결 상태가 표시될 때까지 몇 분 정도 기다려야 할 수 있습니다.

   수집기 그룹 구성을(를) 수행하고 사용자와 수집기 그룹에 구성 변경 사항을 푸시할 때까지 구성 상태 열에는 동기화되지 않음이 표시되고 런타임 상태 열에는 연결 끊김이 표시되며 *CLI* 명령 ***show interface all***는 인터페이스를 *down*으로 표시합니다.
2. 마지막 열에서 통계를 클릭하여 로깅 디스크가 활성화되었는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 11 | 다음 단계...

Log Collector가 방화벽 로그를 수신하려면 먼저 다음을 수행해야 합니다.

1. Panorama에 대한 로그 포워딩을 구성합니다.
2. 수집기 그룹 구성 - M-시리즈 어플라이언스에서 기본 수집기 그룹은 사전 정의되어 있으며 이미 로컬 로그 수집기를 구성원으로 포함합니다. Panorama 가상 어플라이언스에서 Collector Group을 추가하고 로컬 Log Collector를 구성원으로 추가해야 합니다. 두 모델 모두에서 로그 포워딩을 위해 로컬 로그 수집기에 방화벽을 할당합니다.

   방화벽 로그 수집을 시작하려면 먼저 로그 수집기를 수집기 그룹에 추가해야 합니다. ElasticSearch 상태는 저하됨으로 표시되며 로그 수집기는 수집기 그룹에 추가될 때까지 로그를 수집할 수 없습니다.
3. 관리형 수집기 상태 모니터링을(를) 수행하여 로그 수집에 영향을 미치는 문제가 발생할 경우 이를 식별하고 해결합니다.

 ©2024 Palo Alto Networks, Inc.

관리형 수집기 상태 모니터링

관리형 로그 수집기의 상태를 모니터링하여 로그 수집에 영향을 주는 문제를 식별하고 해결합니다. 로그 수집기 상태는 중요한 로그 수집기 프로세스의 상태를 기반으로 하며 각 로그 수집 프로세스의 전반적인 상태와 상태를 모두 볼 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 관리형 수집기 구성.

STEP 3 | 수집기 그룹 구성.

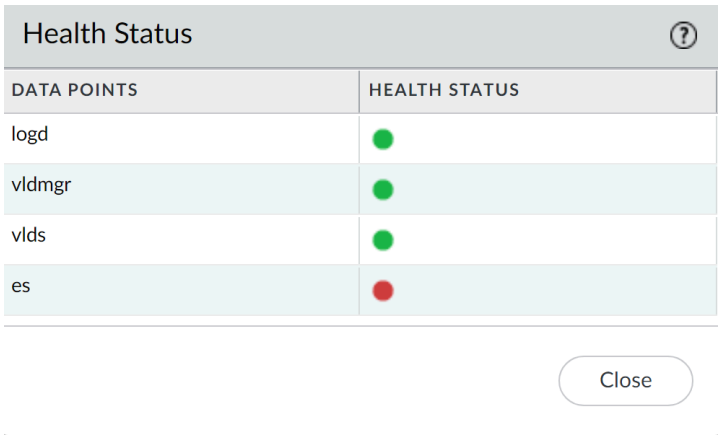
STEP 4 | **Panorama** > 관리형 수집기를 선택하고 상태 열로 이동합니다.

STEP 5 | 로그 수집기의 전반적인 상태를 검토합니다.

녹색 원(●)은 로그 수집기가 정상임을 나타내고 빨간색 원(●)은 하나 이상의 로그 수집 프로세스의 상태가 저하되었음을 나타냅니다.

STEP 6 | 상태 세부 정보를 보고 각 로그 수집 프로세스의 상태를 봅니다.

- **logd** - 관리형 방화벽에서 수신한 로그를 수집하고 수집된 로그를 vldmgr로 전송하는 프로세스입니다.
- **vldmgr** - vld 프로세스 관리를 담당하는 프로세스입니다.
- **vlds** - 개별 로깅 디스크 관리, 로깅 디스크에 로그 쓰기, ElasticSearch에 로그 수집을 담당하는 프로세스입니다.
- **es**- 로그 수집기에서 실행되는 ElasticSearch 프로세스입니다.



 ©2024 Palo Alto Networks, Inc.

전용 로그 수집기에 대한 인증 구성

세분화된 인증 매개변수로 로컬 관리 사용자를 구성하고 권한 부여 및 인증을 위해 RADIUS, TACAS+ 또는 LDAP를 활용하여 전용 로그 수집기에 대한 향상된 인증을 생성 및 구성합니다.

Panorama에서 관리자를 구성하고 푸시하면 전용 로그 수집기의 기존 관리자를 Panorama에서 구성한 관리자로 덮어씁니다.

Panorama에서 생성된 관리자 계정은 나중에 전용 로그 수집기로 가져와 Panorama에서 관리됩니다.

전용 로그 수집기에 대한 관리 계정을 구성할 때 수퍼유저 관리자만 지원됩니다. 다른 관리자 역할 유형을 가진 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

(RADIUS 및 TACAS+) 수퍼유저 관리자만 전용 로그 수집기에 대한 관리 계정을 구성할 때 지원됩니다. 다른 관리자 역할 유형을 가진 원격, 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

- 전용 로그 수집기에 대한 관리 계정 구성
- 전용 로그 수집기에 대한 RADIUS 인증 구성
- 전용 로그 수집기에 대한 TACACS+ 인증 구성
- 전용 로그 수집기에 대한 LDAP 인증 구성

전용 로그 수집기에 대한 관리 계정 구성

Panorama™ 관리 서버에서 관리할 전용 로그 수집기에 대한 세분화된 인증 매개변수를 사용하여 관리자를 한 명 이상 생성합니다. 또한 전용 로그 수집기의 CLI에서 직접 구성할 수 있는 Panorama에서 로컬 관리자를 구성할 수 있습니다. 그러나 전용 로그 수집기에 새 구성 변경 사항을 푸시하면 전용 로그 수집기에 대해 구성된 관리자가 기존 로컬 관리자를 덮어씁니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 관리형 수집기 구성.

STEP 3 | (선택 사항) 전용 로그 수집기 CLI에 액세스하는 관리자의 로그인 자격 증명을 확인하는 인증 서비스를 정의하도록 인증 프로파일을 구성합니다.

STEP 4 | 필요에 따라 하나 이상의 관리자 계정을 구성합니다.

Panorama에서 생성된 관리자 계정은 나중에 전용 로그 수집기로 가져와 Panorama에서 관리됩니다.

전용 로그 수집기에 대한 관리 계정을 구성할 때 수퍼유저 관리자만 지원됩니다. 다른 관리자 역할 유형을 가진 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 전용 로그 수집기에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 수집기를 선택하고 이전에 추가한 전용 로그 수집기를 선택합니다.
2. (선택 사항) 이전 단계에서 구성한 인증 프로파일을 선택합니다.
3. 전용 로그 수집기에 대한 인증 타임아웃 구성을 구성합니다.
   1. 전용 로그 수집기 CLI에서 사용자가 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 전용 로그 수집기가 사용자 계정을 잠그는 잠금 시간(분)을 입력하십시오.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 전용 로그 수집기에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. 전용 로그 수집기 관리자를 추가합니다.

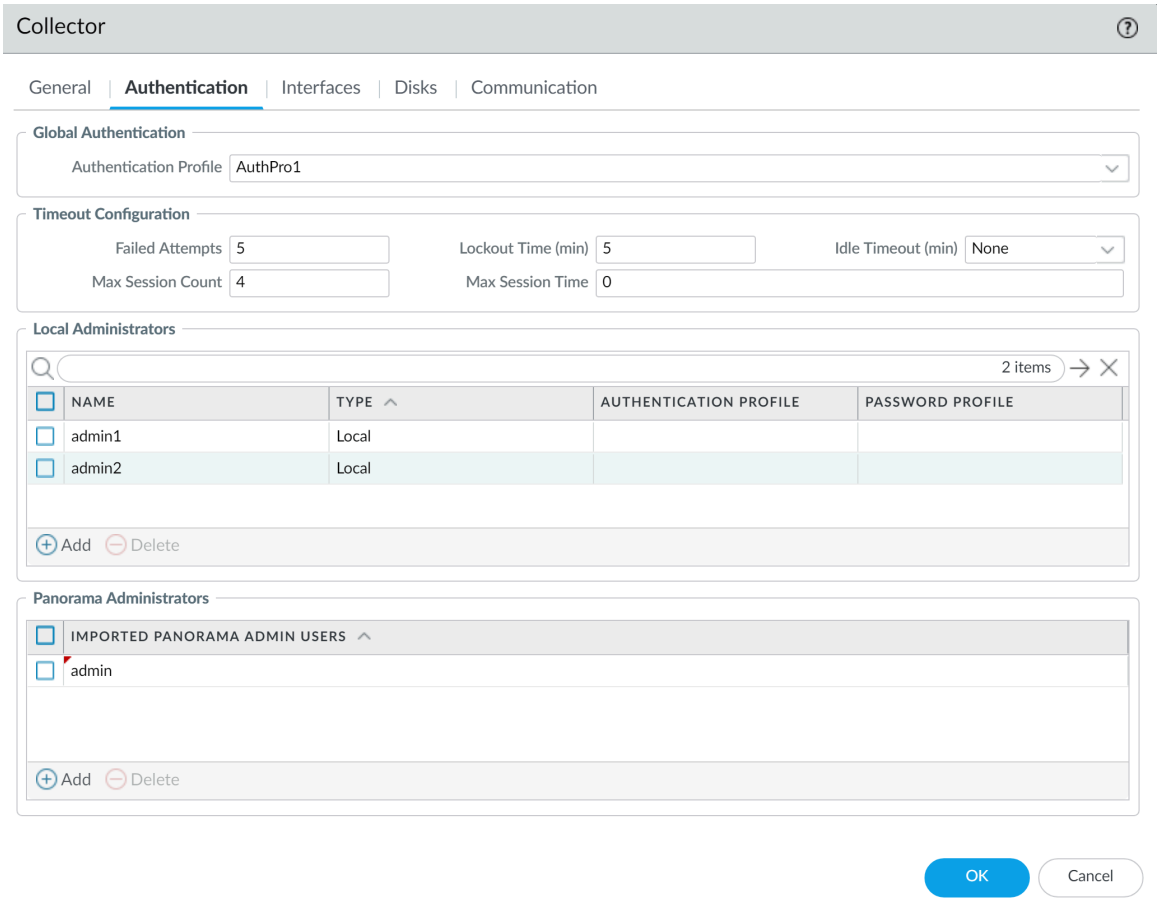
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. 전용 로그 수집기에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 전용 로그 수집기에 따라 다르며 이 테이블에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 Dedicated Log Collector로 가져옵니다.

5. 확인을 클릭하여 전용 로그 수집기 인증 구성을 저장합니다.



STEP 6 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 7 | 전용 로그 수집기의 Panorama CLI에 로그인을(를) 통해, 로컬 관리자를 사용하여 전용 로그 수집기에 성공적으로 액세스할 수 있는지 확인합니다.

전용 로그 수집기에 대한 RADIUS 인증 구성

RADIUS 서버를 사용하여 전용 로그 수집기 CLI에 대한 관리 액세스를 인증합니다. RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama™ 관리 서버에서 설정을 재구성하는 것보다 훨씬 쉽습니다.

©2024 Palo Alto Networks, Inc.

Palo Alto Networks RADIUS 사전을 *RADIUS* 서버로 가져와 *Panorama*와 *RADIUS* 서버 간의 통신에 필요한 인증 속성을 정의할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 관리형 수집기 구성.

STEP 3 | RADIUS 인증을 구성합니다.

전용 로그 수집기에 대한 관리 계정을 구성할 때 수퍼유저 관리자만 지원됩니다. 다른 관리자 역할 유형을 가진 원격, 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

1. RADIUS 서버 프로파일을 추가합니다.

   프로파일은 전용 로그 수집기가 RADIUS 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server Profiles** > **RADIUS**를 선택하고 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 1–20 범위).
   4. 전용 로그 수집기가 RADIUS 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

      RADIUS 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.

   5. 각 RADIUS 서버를 추가하고 다음을 입력합니다.
      1. 서버를 식별하기 위한 이름입니다.
      2. **RADIUS** 서버 IP 주소 또는 FQDN.
      3. **Secret/Confirm Secret**(사용자 이름과 암호를 암호화하는 키).
      4. 인증 요청을 위한 서버 포트(기본값은 1812).
   6. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. RADIUS 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
   2. 인증 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **RADIUS**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. **RADIUS**에서 사용자 그룹 검색을 선택하여 RADIUS 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 전용 로그 수집기에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 수집기를 선택하고 이전에 추가한 전용 로그 수집기를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. 전용 로그 수집기에 대한 인증 타임아웃 구성을 구성합니다.

   1. 전용 로그 수집기 CLI에서 사용자가 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 전용 로그 수집기가 사용자 계정을 잠그는 잠금 시간(분)을 입력하십시오.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 전용 로그 수집기에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. 전용 로그 수집기 관리자를 추가합니다.

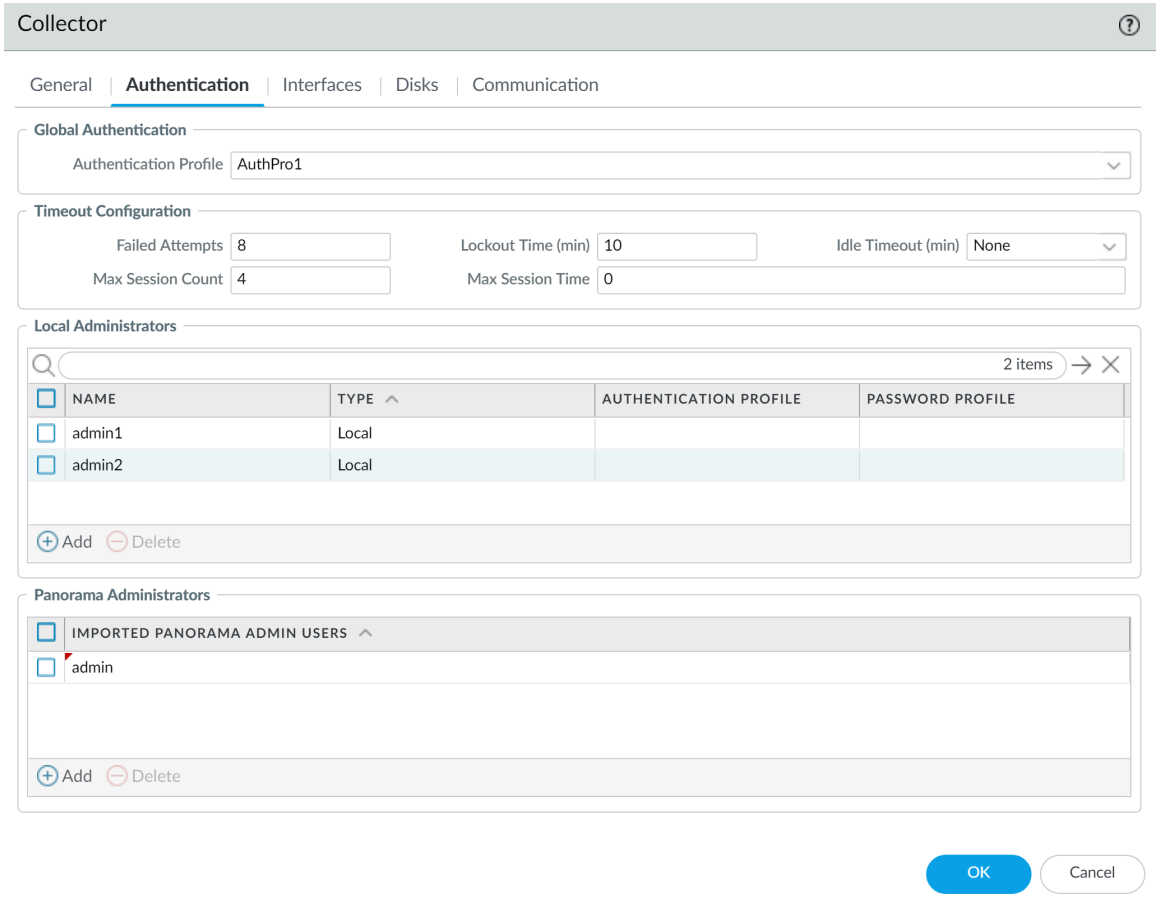
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. 전용 로그 수집기에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 전용 로그 수집기에 따라 다르며 이 테이블에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 Dedicated Log Collector로 가져옵니다.

5. 확인을 클릭하여 전용 로그 수집기 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | 전용 로그 수집기의 Panorama CLI에 로그인을(를) 통해, 로컬 관리자를 사용하여 전용 로그 수집기에 성공적으로 액세스할 수 있는지 확인합니다.

전용 로그 수집기에 대한 TACACS+ 인증 구성

TACACS+ 서버를 사용하여 전용 로그 수집기 CLI에 대한 관리 액세스를 인증할 수 있습니다. TACACS+ 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

©2024 Palo Alto Networks, Inc.

STEP 2 | 관리형 수집기 구성.

STEP 3 | TACACS+ 인증을 구성합니다.

전용 로그 수집기에 대한 관리 계정을 구성할 때 수퍼유저 관리자만 지원됩니다. 다른 관리자 역할 유형을 가진 원격, 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

1. TACACS+ 서버 프로파일을 추가합니다.

   프로파일은 전용 로그 수집기가 TACACS+ 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server Profiles** > **TACACS+**를 선택한 다음 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).
   4. Panorama가 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.
   5. TACACS+ 서버가 해당 프로토콜을 지원하는 경우 **CHAP**를 선택하십시오. **PAP**보다 더 안전합니다.
   6. 각 TACACS+ 서버를 추가하고 서버를 식별할

      1. 이름을 입력합니다.
      2. **TACACS+** 서버 IP 주소 또는 FQDN.
      3. 암호/암호 확인(사용자 이름과 암호를 암호화하는 키).
      4. 인증 요청을 위한 서버 포트(기본값은 49).
   7. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택한 다음 프로파일을 추가합니다.
   2. 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **TACACS+**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집하려면 TACACS+에서 사용자 그룹 검색을 선택합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 전용 로그 수집기에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 수집기를 선택하고 이전에 추가한 전용 로그 수집기를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. 전용 로그 수집기에 대한 인증 타임아웃 구성을 구성합니다.

   1. 전용 로그 수집기 CLI에서 사용자가 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 전용 로그 수집기가 사용자 계정을 잠그는 잠금 시간(분)을 입력하십시오.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 전용 로그 수집기에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. 전용 로그 수집기 관리자를 추가합니다.

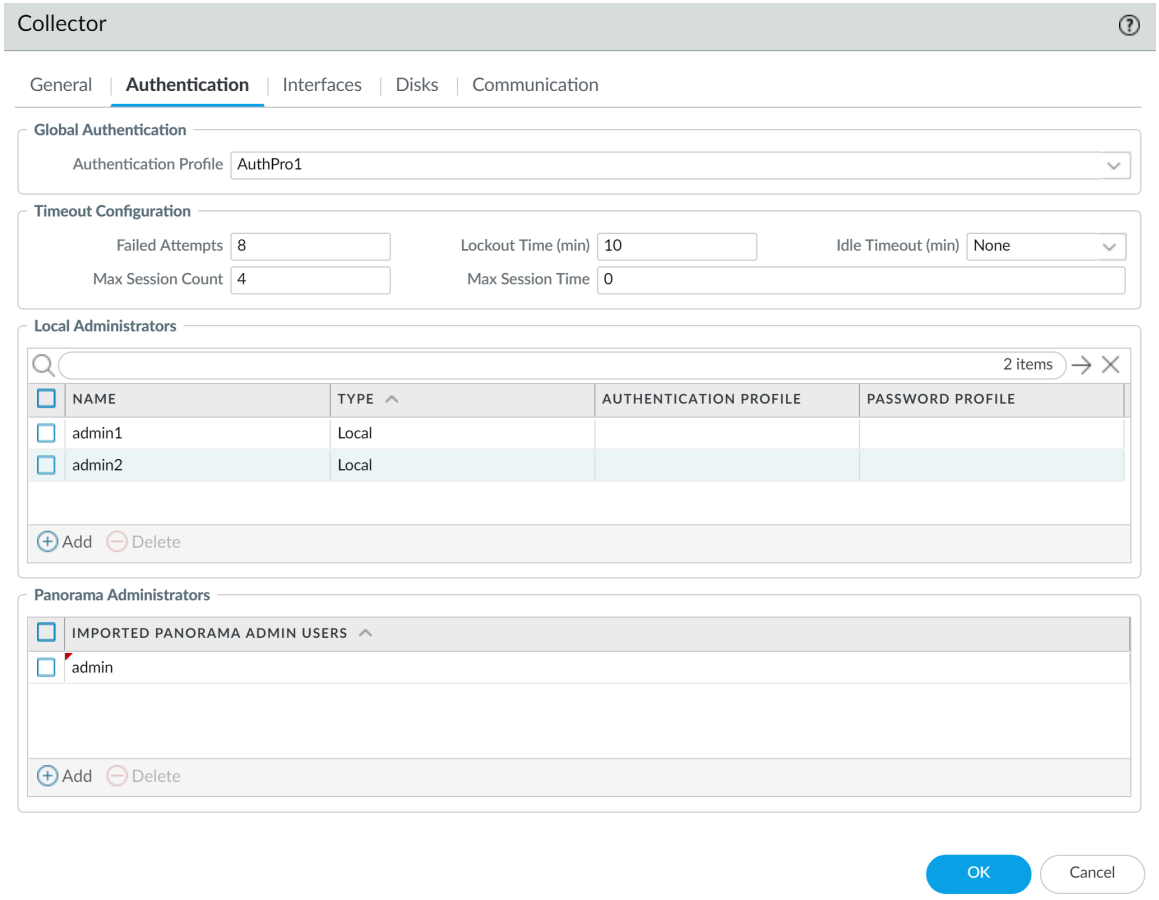
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. 전용 로그 수집기에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 전용 로그 수집기에 따라 다르며 이 테이블에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 Dedicated Log Collector로 가져옵니다.

5. 확인을 클릭하여 전용 로그 수집기 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | 전용 로그 수집기의 Panorama CLI에 로그인을(를) 통해, 로컬 관리자를 사용하여 전용 로그 수집기에 성공적으로 액세스할 수 있는지 확인합니다.

전용 로그 수집기에 대한 LDAP 인증 구성

LDAP를 사용하여 전용 로그 수집기 웹 인터페이스에 액세스하는 최종 사용자를 인증할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 관리형 수집기 구성.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | LDAP 서버 프로파일을 추가합니다.

프로파일은 전용 로그 수집기가 LDAP 서버에 연결하는 방법을 정의합니다.

전용 로그 수집기에 대한 관리 계정을 구성할 때 수퍼유저 관리자만 지원됩니다. 다른 관리자 역할 유형을 가진 로컬 또는 *Panorama* 관리자는 지원되지 않습니다.

1. **Panorama** > 서버 프로파일 > **LDAP** 및 서버 프로파일 추가를 선택합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. LDAP 서버를 추가합니다(최대 4개). 각 서버에 대해 이름(서버 식별), **LDAP** 서버 IP 주소 또는 FQDN 및 서버 포트(기본값 389)를 입력합니다.

   FQDN 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소에 대한 변경 사항을 적용해야 합니다.
4. 서버 유형을 선택합니다.
5. 기본 **DN**을 선택합니다.

   디렉터리의 기본 DN을 식별하려면 **Active Directory** 도메인 및 트러스트 Microsoft 관리 콘솔 스냅인을 열고 최상위 도메인의 이름을 사용합니다.
6. 바인딩 **DN** 및 암호를 입력하여 인증 서비스에서 방화벽을 인증할 수 있도록 합니다.

   Bind DN 계정에는 *LDAP* 디렉토리를 읽을 수 있는 권한이 있어야 합니다.
7. 바인딩 타임아웃 및 검색 타임아웃(초)을 입력합니다. 기본값은 모두 30입니다.
8. 재시도 간격(초)을 입력합니다(기본값은 60).
9. (선택 사항) 엔드포인트가 디렉터리 서버와의 보다 안전한 연결을 위해 SSL 또는 TLS를 사용하도록 하려면 **SSL/TLS** 보안 연결 필요(기본적으로 활성화됨) 옵션을 활성화합니다. 엔드포인트가 사용하는 프로토콜은 서버 포트에 따라 다릅니다.
   - 389(기본값) - TLS(특히 전용 로그 수집기는 초기 일반 텍스트 연결을 TLS로 업그레이드하는 StartTLS 작업을 사용합니다.)
   - 636—SSL
   - 기타 포트 - 전용 로그 수집기는 먼저 TLS 사용을 시도합니다. 디렉터리 서버가 TLS를 지원하지 않는 경우 전용 로그 수집기는 SSL로 대체됩니다.
10. (선택 사항) 보안을 강화하려면 SSL/TLS 연결에 대해 디렉터리 서버가 제공하는 인증서를 엔드포인트에서 확인할 수 있도록 **SSL** 세션에 대한 서버 인증서 확인 옵션을 활성화합니다. 확인을 활성화하려면 **SSL/TLS** 보안 연결 필요 옵션도 활성화해야 합니다. 확인이 성공하려면 인증서가 다음 조건 중 하나를 충족해야 합니다.
    - Panorama 인증서 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서 > 디바이스 인증서. 필요한 경우 인증서를 Panorama로 가져옵니다.
    - 인증서 서명자는 신뢰할 수 있는 인증 기관 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서.
11. 확인을 클릭하여 서버 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 전용 로그 수집기에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 수집기를 선택하고 이전에 추가한 전용 로그 수집기를 선택합니다.
2. 전용 로그 수집기에 대한 인증 타임아웃 구성을 구성합니다.
   1. 전용 로그 수집기 CLI에서 사용자가 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 전용 로그 수집기가 사용자 계정을 잠그는 잠금 시간(분)을 입력하십시오.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃**(**분**)**을 입력합니다.
   4. 최대 세션 수를 입력하여 전용 로그 수집기에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
3. 전용 로그 수집기 관리자를 추가합니다.

   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

   - 로컬 관리자를 구성합니다.

     전용 로그 수집기에 고유한 새 관리자를 구성합니다. 이러한 관리자는 생성된 전용 로그 수집기에 따라 다르며 이 테이블에서 관리자를 관리합니다.

     1. 한 명 이상의 새 로컬 관리자를 추가하십시오.
     2. 로컬 관리자의 이름을 입력합니다.
     3. 이전에 생성한 인증 프로파일을 할당합니다.

        LDAP 인증 프로파일은 개별 로컬 관리자에 대해서만 지원됩니다.

     4. 인증을 위해 공개 키 파일을 가져오려면 공개 키 인증**(SSH)** 사용을 활성화(선택)합니다.
     5. 암호 프로파일을 선택하여 만료 매개변수를 설정합니다.
   - 기존 Panorama 관리자 가져오기

     Panorama에 구성된 기존 관리자를 가져옵니다. 이러한 관리자는 Panorama에서 구성 및 관리되며 전용 로그 수집기로 가져옵니다.

     1. 기존 Panorama 관리자 추가
4. 확인을 클릭하여 전용 로그 수집기 인증 구성을 저장합니다.

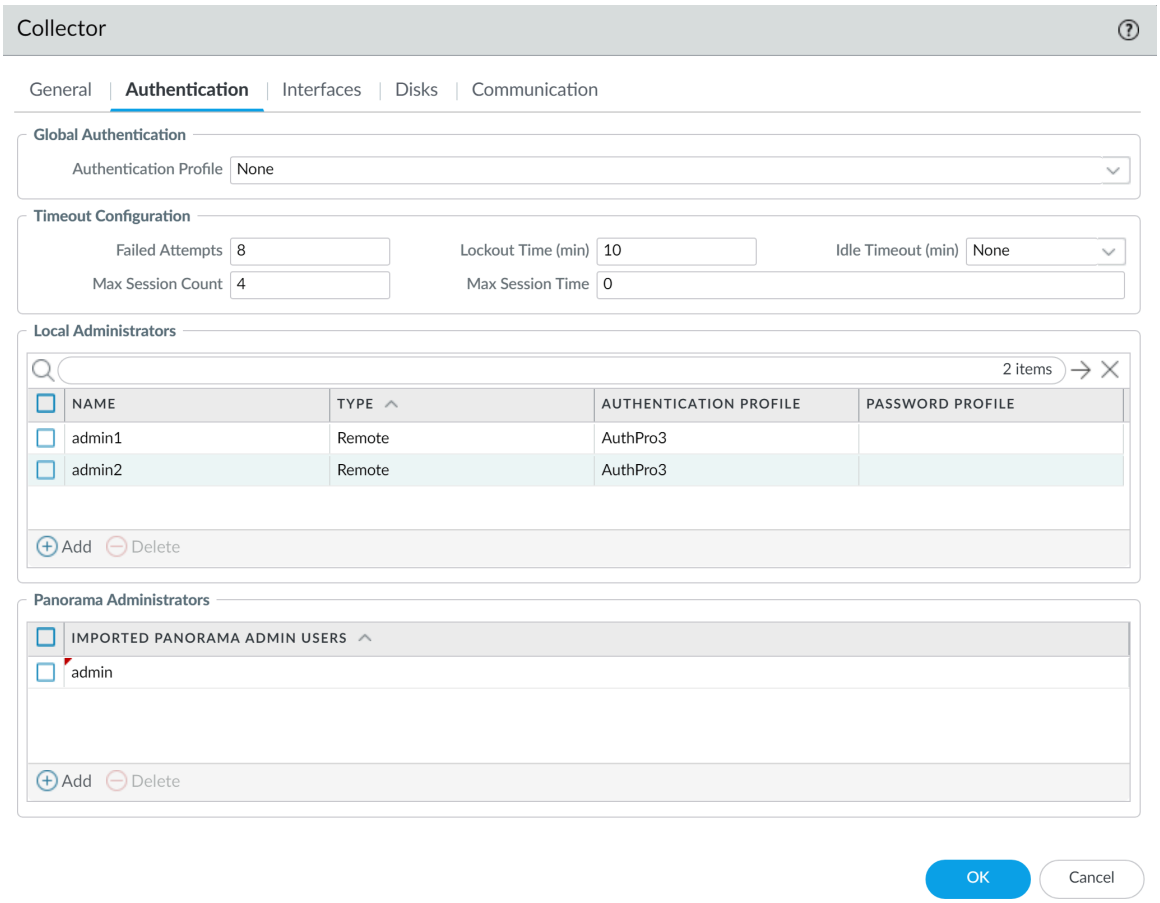
 ©2024 Palo Alto Networks, Inc.

STEP 5 | 전용 로그 수집기에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 수집기를 선택하고 이전에 추가한 전용 로그 수집기를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.
3. 전용 로그 수집기에 대한 인증 타임아웃 구성을 구성합니다.
   1. 전용 로그 수집기 CLI에서 사용자가 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 전용 로그 수집기가 사용자 계정을 잠그는 잠금 시간(분)을 입력하십시오.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 전용 로그 수집기에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. 전용 로그 수집기 관리자를 추가합니다.

   관리자(**admin**)를 로컬 관리자로 추가하거나 불러온 Panorama 관리자로 추가해야 합니다. 둘 다 할 수는 없습니다. 관리자가 추가되지 않았거나 관리자가 로컬 관리자와 불러온 Panorama 관리자 모두로 추가된 경우 관리형 수집기에 대한 푸시가 실패합니다.
   1. 전용 로그 수집기에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 전용 로그 수집기에 따라 다르며 이 테이블에서 관리자를 관리합니다.
   2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 Dedicated Log Collector로 가져옵니다.
5. 확인을 클릭하여 전용 로그 수집기 인증 구성을 저장합니다.

 ©2024 Palo Alto Networks, Inc.



STEP 6 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 7 | 전용 로그 수집기의 Panorama CLI에 로그인을(를) 통해, 로컬 관리자를 사용하여 전용 로그 수집기에 성공적으로 액세스할 수 있는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

수집기 그룹 관리

수집기 그룹은 방화벽 로그를 수집하기 위한 단일 논리 단위로 작동하는 1~16개의 로그 수집기입니다. 방화벽이 로그 수집기에 성공적으로 로그를 보내려면 수집기 그룹에 하나 이상의 로그 수집기를 할당해야 합니다. 구성된 수집기 그룹이 없거나 수집기 그룹에 할당된 로그 수집기가 없는 경우 방화벽 로그가 삭제됩니다. 다중 로그 수집기로 수집기 그룹을 구성하여 로그 중복성을 보장하거나 단일 로그 수집기의 용량을 초과하는 로깅 속도를 수용할 수 있습니다(Panorama 모델 참조). 위험 및 권장되는 완화 방법을 이해하려면 여러 로그 수집기가 있는 수집기 그룹에 대한 주의 사항을 참조하세요.

M-700, M-600, M-500, M-300 및 M-200 어플라이언스에는 사전 정의된 로컬 로그 수집기를 포함하는 사전 정의된 수집기 그룹이 있습니다. 이름(기본값)을 제외하고 사전 정의된 수집기 그룹의 모든 설정을 편집할 수 있습니다.

*Collector Group*을 삭제하면 로그가 손실됩니다.

*Palo Alto Networks*는 *Panorama*가 전용 로그 수집기를 관리하는지의 여부와 관계없이 *Panorama* 관리 서버에 사전 정의된 로그 수집기 및 수집기 그룹을 유지할 것을 권장합니다.

M-시리즈 어플라이언스를 *Panorama* 모드에서 로그 수집기 모드로 전환하면 어플라이언스에서 사전 정의된 수집기 그룹 및 로그 수집기가 손실됩니다. 그런 다음 M 시리즈 어플라이언스를 로그 수집기로 설정하고 *Panorama*에 관리 수집기로 추가하고 관리 수집기를 포함하도록 수집기 그룹을 구성해야 합니다.

- 수집기 그룹 구성
- 로그 수집기 간에 사용자 지정 인증서로 인증 구성
- 로그 수집기를 다른 수집기 그룹으로 이동
- 수집기 그룹에서 방화벽 제거

수집기 그룹 구성

수집기 그룹을 구성하기 전에 각 그룹에 단일 로그 수집기 또는 여러 로그 수집기(최대 16개)가 있는지의 여부를 결정하십시오. 여러 로그 수집기가 있는 수집기 그룹은 더 높은 로깅 속도와 로그 중복성을 지원하지만 다음 요구 사항이 있습니다.

- 모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 파노라마 모델인 모든 M-700 기기, 모든 M-600 기기, 모든 M-500 기기, 모든 M-300 기기, 모든 M-200 기기 또는 모든 파노라마 가상 어플라이언스에서 실행되어야 합니다.
- 로그 중복성은 각 로그 수집기에 동일한 수의 로깅 디스크가 있는 경우에만 사용할 수 있습니다. 로그 수집기에 디스크를 추가하려면 M-시리즈 어플라이언스에서 스토리지 늘리기를 참조하십시오.
- (모범 사례) 동일한 수집기 그룹의 모든 로그 수집기는 동일한 LAN(Local Area Network)에 있어야 합니다. 네트워크 중단이 훨씬 더 일반적이고 로그 데이터 손실을 초래할 수 있으므로 동일하거나 다른 WAN(광역 네트워크)의 로그 수집기를 동일한 수집기 그룹에 추가하지 마십시오. 또한 Panorama가 필요할 때 신속하게 로그 수집기를 쿼리할 수 있도록 동일한 수집기 그룹의 로그 수집기를 서로 물리적으로 근접하게 두는 것이 좋습니다.

©2024 Palo Alto Networks, Inc.

방화벽 로그 수집을 시작하려면 로그 수집기를 수집기 그룹에 추가하고 수집기 그룹 구성을 로그 수집기에 푸시해야 합니다. 이렇게 하지 않을 경우 ElasticSearch 상태는 저하됨으로 표시되고 로그 수집기는 수집기 그룹에 추가될 때까지 로그를 수집할 수 없습니다.

STEP 1 | Collector Group을 구성하기 전에 다음 작업을 수행하십시오.

1. 수집기 그룹에 할당할 각 방화벽에 대해 관리되는 디바이스로 방화벽을 추가합니다.
2. 수집기 그룹에 할당할 각 로그 수집기에 대해 관리 수집기를 구성합니다.

STEP 2 | 수집기 그룹을 추가합니다.

1. Panorama 웹 인터페이스에 액세스하고**Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 추가하거나 기존 그룹을 편집합니다.
2. 수집기 그룹을 추가하는 경우 수집기 그룹의 이름을 입력합니다.

   기존 수집기 그룹의 이름은 변경할 수 없습니다.
3. 수집기 그룹이 방화벽 로그를 보관할 최소 보존 기간(1~2,000일)을 입력합니다.

   기본적으로 필드는 비어 있습니다. 즉, 수집기 그룹이 로그를 무기한 보관합니다.
4. 수집기 그룹 구성원 목록에 로그 수집기(1 ~ 16)를 추가합니다.
5. (권장) 단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화합니다.

   중복성은 하나의 로그 수집기를 사용할 수 없게 되는 경우에도 로그가 손실되지 않도록 합니다. 각 로그에는 두 개의 사본이 있으며 각 사본은 다른 로그 수집기에 상주합니다. 예를 들어 수집기 그룹에 두 개의 로그 수집기가 있는 경우 로그는 두 로그 수집기에 모두 기록됩니다.

   중복성을 활성화하면 더 많은 로그가 생성되므로 더 많은 저장 용량이 필요하므로 저장 용량이 절반으로 줄어듭니다. Collector Group의 공간이 부족하면 오래된 로그를 삭제합니다. 또한 중복성은 수집기 그룹에서 로그 처리 트래픽을 두 배로 하여 각 로그 수집기가 수신하는 각 로그의 복사본을 배포해야 하므로 최대 로깅 속도를 절반으로 줄입니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 수집기 그룹에 로그 수집기 및 방화벽을 할당합니다.

1. 디바이스 로그 포워딩을 선택하고 방화벽에 대한 로그 포워딩 기본 설정 목록 추가를 선택합니다.

   로그 데이터는 별도의 TCP 채널을 통해 포워딩됩니다. 로그 포워딩 기본 설정을 추가하면 로그 데이터를 포워딩하기 위한 별도의 TCP 연결을 생성할 수 있습니다.

   기본 설정 목록은 로그 수집기가 방화벽에서 로그를 수신하는 순서를 결정합니다. 로그 포워딩 기본 설정 목록이 할당되지 않은 경우 다음 시나리오 중 하나가 발생할 수 있습니다.

   - *Panorama*가 관리 전용 모드인 경우 *Panorama*는 모든 수신 로그를 삭제합니다.
   - *Panorama*가 *Panorama* 모드에 있을 때 로컬 로그 수집기가 관리 수집기로 구성되지 않은 경우 *Panorama*는 들어오는 모든 로그를 삭제합니다.
   - *Panorama*가 *Panorama* 모드일 때 로컬 *Log Collector*가 관리형 수집기로 구성되어 있으면 들어오는 로그가 수신되지만 모든 관리형 방화벽이 로그를 다른 사용 가능한 로그 수집기에 재배포하기 전에 먼저 로컬 *Log Collector*에 포워딩하기 때문에 *Panorama*가 병목 현상으로 작용할 수 있습니다.

   1. 디바이스 섹션에서 방화벽 목록을 수정하고 확인을 클릭합니다.
   2. 수집기 섹션에서 기본 설정 목록에 로그 수집기를 추가합니다.

      2단계에서 중복성을 활성화한 경우 최소 두 개의 로그 수집기를 추가하는 것이 좋습니다. 여러 Log Collector를 할당하는 경우 첫 번째 Log Collector가 기본이 됩니다. 기본을 사용할 수 없게 되면 방화벽은 목록의 다음 로그 수집기로 로그를 보냅니다. 로그 수집기의 우선 순위를 변경하려면 로그 수집기를 선택하고 위로 이동(높은 우선 순위) 또는 아래로 이동(낮은 우선 순위)을 선택합니다.
   3. 확인을 클릭합니다.

STEP 4 | 각 로그 유형에 대한 저장 용량(로그 할당량) 및 만료 기간을 정의합니다.

1. 일반 탭으로 돌아가서 로그 스토리지 값을 클릭하십시오.

   필드에 *0MB*가 표시되면 로깅을 위해 디스크 쌍을 활성화하고 변경 사항을 커밋했는지 확인합니다(관리되는 수집기 구성, 디스크 탭 참조).
2. 각 로그 유형에 대한 로그 저장소 할당량**(%)**을 입력합니다.
3. 각 로그 유형(1 ~ 2,000)에 대한 최대 일수(만료 기간)를 입력합니다.

   기본적으로 필드는 비어 있으므로 로그가 만료되지 않습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 변경 사항을 커밋하고 확인합니다.

1. 커밋 > 커밋 및 푸시를 선택한 다음, Panorama 및 구성한 수집기 그룹에 대한 변경 사항 커밋 및 푸시를 선택합니다.
2. 수집기 그룹의 로그 수집기가 다음과 같은지 확인하려면 **Panorama** > 관리형 수집기를 선택합니다.
   - **Panorama**에 연결됨 - 연결됨 열에는 로그 수집기가 Panorama에 연결되었음을 나타내는 확인 표시 아이콘이 표시됩니다.
   - **Panorama**와 동기화됨 - 구성 상태 열은 로그 수집기가 Panorama와 ### #(녹색 아이콘) 또는 ##### ##(빨간색 아이콘)인지의 여부를 나타냅니다.

STEP 6 | 네트워크 리소스에 대한 연결 문제 해결을(를) 수행하여 방화벽이 로그 수집기에 성공적으로 연결되었는지 확인합니다.

STEP 7 | 다음 단계...

1. Panorama에 대한 로그 포워딩을 구성합니다.

   Collector Group은 Panorama로 포워딩하도록 방화벽을 구성할 때까지 방화벽 로그를 수신하지 않습니다.
2. (선택 사항) Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.

   로그를 별도의 대상(예: syslog 서버)으로 포워딩하도록 각 수집기 그룹을 구성할 수 있습니다.

로그 수집기 간에 사용자 지정 인증서로 인증 구성

Log Collector 간의 통신을 위한 사용자 지정 인증서를 구성하려면 다음 절차를 완료하십시오. 서버 및 클라이언트 역할이 동적으로 선택되므로 수집기 그룹의 각 로그 수집기에서 보안 서버 통신 및 보안 클라이언트 통신을 구성해야 합니다. 사용자 지정 인증서를 사용하여 로그 수집기 그룹 구성원 간의 상호 인증을 보장하는 고유한 신뢰 체인을 생성합니다.

사용자 지정 인증서 사용에 대한 자세한 내용은 SSL/TLS 연결이 상호 인증되는 방법을 참조하십시오.

STEP 1 | 각 로그 수집기에 대한 키 쌍 및 인증 기관(CA) 인증서를 가져옵니다.

STEP 2 | CA 인증서를 가져와서 클라이언트 로그 수집기의 ID, 서버 키 쌍 및 수집기 그룹의 각 로그 수집기에 대한 클라이언트 키 쌍을 확인합니다.

1. **Panorama** > 인증서 관리 > 인증서 > 가져오기를 선택합니다.
2. CA 인증서, 서버 키 쌍 및 클라이언트 키 쌍을 가져옵니다.
3. 각 로그 수집기에 대해 단계를 반복합니다.

STEP 3 | 보안 서버 통신을 위해 루트 CA 및 중간 CA를 포함하는 인증서 프로파일을 구성합니다. 이 인증서 프로파일은 로그 수집기 간의 인증을 정의합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

   인증서 프로파일의 일부로 중간 CA를 구성하는 경우 루트 CA도 포함해야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 보안 클라이언트 통신을 위한 인증서 프로파일을 구성합니다. 각 클라이언트 로그 수집기에서 이 프로파일을 개별적으로 구성하거나 Panorama™에서 관리되는 로그 수집기로 구성을 푸시할 수 있습니다.

클라이언트 인증서에 *SCEP*를 사용하는 경우 인증서 프로파일 대신 SCEP 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

STEP 5 | SSL/TLS 서비스 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. 로그 수집기가 SSL/TLS 서비스에 사용하는 인증서 및 프로토콜을 정의하도록 SSL/TLS 서비스 프로파일을 구성합니다.

STEP 6 | 모든 로그 수집기에 사용자 지정 인증서를 배포한 후 사용자 지정 인증서 인증을 시행합니다.

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 선택합니다.
2. 일반 탭에서 보안 간 **LC** 통신을 활성화합니다.

   보안 LC 간 통신을 활성화하고 수집기 그룹에 로컬 로그 수집기가 포함된 경우 로컬 Panorama의 로그 수집기가 **Panorama** > **Secure** 통신 설정의 보안 클라이언트 구성을 사용하고 있다는 링크가 나타나야 합니다. 이 링크를 클릭하여 통신 보안 설정 대화 상자를 열고 로컬 로그 수집기에 대한 보안 서버 및 보안 클라이언트 설정을 구성할 수 있습니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

STEP 7 | 각 로그 수집기에서 보안 서버 통신을 구성합니다.

1. 전용 로그 수집기에 대한 **Panorama** > 관리 수집기 또는 **Panorama** > 설정 > 관리를 선택하고 로컬 로그 수집기에 대한 보안 통신 설정을 편집합니다.
2. 전용 로그 수집기의 경우 로그 수집기를 클릭하고 통신을 선택합니다.
3. 보안 서버 통신 사용자 지정 기능을 활성화합니다.
4. SSL/TLS 서비스 프로파일 드롭다운에서 **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 로그 수집기 간의 모든 SSL 연결에 적용됩니다.
5. 드롭다운에서 인증서 프로파일을 선택합니다.
6. 사용자 지정 인증서만 비활성화(선택 취소)되었는지 확인합니다. 이를 통해 사용자 지정 인증서를 구성하는 동안 사전 정의된 인증서를 사용하여 로그 수집기 간 통신을 계속할 수 있습니다.
7. 연결 해제 대기 시간(로그 수집기가 다른 로그 수집기와의 연결을 끊고 다시 설정하기 전에 대기하는 시간(분))을 설정합니다. 이 필드는 기본적으로 비어 있습니다(범위는 0~44,640).
8. (선택 사항) 권한 부여 목록을 구성합니다. 권한 부여 목록은 인증서 인증 이상의 보안 계층을 추가합니다. 인증 목록은 클라이언트 인증서 주체 또는 주체 대체 이름을 확인합니다. 클라이언트 인증서와 함께 제공된 주체 또는 주체 대체 이름이 인증 목록의 식별자와 일치하지 않으면 인증이 거부됩니다.

   1. 권한 부여 목록을 추가합니다.

 ©2024 Palo Alto Networks, Inc.

2. 인증서 프로파일에 구성된 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
3. 식별자가 ##인 경우 일반 이름을 입력하고 식별자가 ## ## ##인 경우 IP 주소, 호스트 이름 또는 이메일을 입력합니다.
4. 확인을 클릭합니다.
5. 권한 부여 목록 확인 옵션을 활성화하여 권한 부여 목록을 적용하도록 Panorama를 구성하십시오.

9. 확인을 클릭합니다.
10. 변경 사항을 커밋합니다.

이러한 변경 사항을 커밋한 후 연결 해제 대기 시간 카운트다운이 시작됩니다. 대기 시간이 끝나면 수집기 그룹의 로그 수집기는 구성된 인증서 없이 연결할 수 없습니다.

STEP 8 | 각 로그 수집기에서 보안 클라이언트 통신을 구성합니다.

1. 전용 로그 수집기에 대한 **Panorama** > 관리 수집기 또는 **Panorama** > 설정 > 관리를 선택하고 로컬 로그 수집기에 대한 보안 통신 설정을 편집합니다.
2. 전용 로그 수집기의 경우 로그 수집기를 클릭하고 통신을 선택합니다.
3. 보안 클라이언트 통신 아래의 해당 드롭다운에서 인증서 유형, 인증서 및 인증서 프로파일을 선택합니다.
4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

로그 수집기를 다른 수집기 그룹으로 이동

M-700, M-600, M-500, M-300, M-200 및 Panorama 가상 어플라이언스는 각 수집기 그룹에 하나 이상의 로그 수집기를 가질 수 있습니다. 수집기 그룹의 로깅 속도 및 로그 스토리지 요구 사항에 따라 수집기 그룹에 로그 수집기를 할당합니다. 수집기 그룹에서 속도와 필요한 스토리지가 증가하는 경우 모범 사례는 M-시리즈 어플라이언스에서 스토리지를 늘리거나 추가 로그 수집기로 수집기 그룹을 구성하는 것입니다. 그러나 일부 배포에서는 수집기 그룹 간에 로그 수집기를 이동하는 것이 더 경제적일 수 있습니다.

로그 수집기가 *Panorama* 모드의 *M-700*, *M-600*, *M-500*, *M-300* 또는 *M-200*에 로컬인 경우 어플라이언스가 고가용성*(HA)* 구성의 수동 피어인 경우에만 이동합니다. *HA* 동기화는 새 수집기 그룹과 연결된 구성을 적용합니다. 활성 *HA* 피어에 로컬인 로그 수집기를 이동하지 마십시오.

모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.

로그 중복성은 각 로그 수집기에 동일한 수의 로깅 디스크가 있는 경우에만 사용할 수 있습니다. 로그 수집기에 디스크를 추가하려면 M-시리즈 어플라이언스에서 스토리지 늘리기를 참조하십시오.

STEP 1 | Panorama 관리에서 로그 수집기를 제거합니다.

 ©2024 Palo Alto Networks, Inc.

1. **Panorama** > 수집기 그룹를 선택한 다음 이동할 로그 수집기가 포함된 수집기 그룹을 편집합니다.
2. 수집기 그룹 구성원 목록에서 로그 수집기를 선택한 다음 삭제합니다.
3. 디바이스 로그 포워딩을 선택한 다음 로그 포워딩 기본 설정 목록에서 이동할 로그 수집기에 할당된 각 방화벽 집합에 대해 다음 단계를 수행합니다.
   1. 디바이스 열에서 로그 수집기에 할당된 방화벽에 대한 링크를 클릭합니다.
   2. 수집기 열에서 로그 수집기를 선택한 다음 삭제합니다.

      방화벽을 재할당하려면 방화벽이 로그를 포워딩할 새 *Log Collector*를 추가합니다.
   3. 확인을 두 번 클릭하여 변경 사항을 저장합니다.
4. **Panorama** > 관리형 수집기를 선택한 다음 이동할 로그 수집기를 선택한 다음 삭제합니다.

STEP 2 | 수집기 그룹을 구성합니다.

새 수집기 그룹에 로그 수집기를 추가하고 로그 수집기에 방화벽을 할당합니다.

수집기 그룹 구성에 변경 사항을 푸시하면 *Panorama*가 로그 수집기 전체에 로그를 재배포하기 시작합니다. 이 프로세스는 로그의 각 테라바이트에 대해 몇 시간이 걸릴 수 있습니다. 재배포 과정에서 최대 로깅 속도가 감소합니다. ***Panorama*** > ***Collector Groups*** 페이지에서 *Log Redistribution State* 열은 프로세스의 완료 상태를 백분율로 나타냅니다.

STEP 3 | 구성한 새 수집기 그룹에 대한 Panorama에 대한 로그 포워딩 구성.

STEP 4 | 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 아직 수행하지 않은 경우 디바이스 그룹, 템플릿 및 수집기 그룹에 변경 사항을 푸시합니다.

수집기 그룹에서 방화벽 제거

레거시 모드에서 Panorama 가상 어플라이언스를 사용하여 전용 로그 수집기를 관리하는 경우 방화벽 로그를 로그 수집기로 포워딩하는 대신 Panorama로 포워딩할 수 있는 옵션이 있습니다. 이러한 경우 수집기 그룹에서 방화벽을 제거해야 합니다. 그러면 방화벽이 자동으로 해당 로그를 Panorama로 포워딩합니다.

방화벽에서 로그 포워딩 기본 설정 목록을 일시적으로 제거하려면 방화벽에서 *CLI*를 사용하여 삭제할 수 있습니다. 그러나 *Panorama*의 *Collector Group* 구성에서 할당된 방화벽을 제거해야 합니다. 그렇지 않으면 다음에 수집기 그룹에 변경 사항을 푸시할 때 할당된 로그 수집기로 로그를 보내도록 방화벽이 재구성됩니다.

STEP 1 | **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 편집합니다.

STEP 2 | 디바이스 로그 포워딩을 선택한 다음 디바이스 목록에서 방화벽을 클릭하고 디바이스 목록을 수정하고 방화벽의 체크박스를 선택 취소하고 확인을 세 번 클릭합니다.

STEP 3 | 커밋 > 커밋 및 푸시를 선택한 다음 방화벽을 제거한 Panorama 및 수집기 그룹에 변경 사항을 커밋 및 푸시합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama에 대한 로그 포워딩 구성

각 방화벽은 기본적으로 로그 파일을 로컬에 저장하며 다른 방화벽에 있는 로그는 표시할 수 없습니다. 따라서 모든 방화벽이 모니터링하는 네트워크 활동에 대한 글로벌 가시성을 확보하려면 모든 방화벽 로그를 Panorama로 포워딩하고 가시성을 위해 Panorama 사용을 수행해야 합니다. 조직의 일부 팀이 작업과 관련된 로그만 모니터링하여 효율성을 높일 수 있는 경우 모든 로그 속성(예: 위협 유형 또는 소스 사용자)을 기반으로 포워딩 필터를 생성할 수 있습니다. 예를 들어 맬웨어 공격을 조사하는 보안 운영 분석가는 유형 속성이 wildfire-virus로 설정된 위협 로그에만 관심이 있을 수 있습니다.

다음 단계에서는 Panorama 템플릿 및 디바이스 그룹을 사용하여 로그를 포워딩하도록 여러 방화벽을 구성하는 방법을 설명합니다.

*Panorama*가 *PAN-OS 7.0* 이전 버전의 소프트웨어를 실행하는 방화벽을 관리하는 경우 *Panorama*가 해당 방화벽이 제출하는 *WildFire* 샘플에 대한 분석 정보를 수집할 수 있는 *WildFire*® 서버를 지정하십시오. *Panorama*는 이 정보를 사용하여 *PAN-OS 7.0*에 도입된 필드 값이 누락된 *WildFire* 제출 로그를 완성합니다. 이전 릴리스를 실행하는 방화벽은 해당 필드를 채우지 않습니다. 서버를 지정하려면 ***Panorama*** > ***Setup*** > ***WildFire***를 선택하고 일반 설정을 편집한 다음 ***WildFire Private Cloud*** 이름을 입력합니다. 기본값은 미국에서 호스팅되는 *WildFire* 클라우드인 ***wildfire-public-cloud***입니다.

방화벽 로그를 외부 서비스(예: *syslog* 서버)로 포워딩할 수도 있습니다. 자세한 내용은 로그 포워딩 옵션을 참조하십시오.

STEP 1 | 로그를 포워딩할 방화벽에 대한 디바이스 그룹을 추가합니다.

Panorama는 로그 포워딩 프로파일을 방화벽으로 푸시하려면 디바이스 그룹이 필요합니다. 새 디바이스 그룹을 생성하거나 기존 디바이스 그룹에 방화벽을 할당합니다.

STEP 2 | 로그를 포워딩할 방화벽에 대한 템플릿을 추가합니다.

Panorama에는 방화벽에 로그 설정을 푸시하는 템플릿이 필요합니다. 새 템플릿을 만들거나 기존 템플릿에 방화벽을 할당합니다.

STEP 3 | 로그 포워딩 프로파일을 생성합니다.

프로파일은 트래픽, 위협, WildFire 제출, URL 필터링, 데이터 필터링, 터널 및 인증 로그의 대상을 정의합니다.

1. 개체 > 로그 포워딩을 선택하고 로그를 포워딩할 방화벽의 디바이스 그룹을 선택한 다음 프로파일을 추가합니다.
2. 로그 포워딩 프로파일을 식별하는 이름을 입력합니다.
3. 하나 이상의 일치 목록 프로파일을 추가합니다.

   프로파일은 로그 쿼리 필터, 포워딩 대상 및 태깅과 같은 자동 작업을 지정합니다. 각 일치 리스트 프로파일에 대해 다음을 수행합니다.

   1. 프로파일을 식별하려면 이름을 입력합니다.
   2. 로그 유형을 선택합니다.
   3. 필터 드롭다운에서 필터 빌더를 선택합니다. 다음을 지정하고 각 쿼리를 추가합니다.

 ©2024 Palo Alto Networks, Inc.

커넥터 로직(및/또는)

로그 속성

포함 또는 제외 논리를 정의하는 연산자

일치시킬 쿼리의 속성 값

4. **Panorama/Strata Logging Service**를 선택합니다.

4. 확인을 클릭하여 로그 포워딩 프로파일을 저장합니다.

STEP 4 | 정책 규칙 및 네트워크 영역에 로그 포워딩 프로파일을 할당합니다.

보안, 인증 및 DoS 보호 규칙은 로그 포워딩을 지원합니다. 이 예에서는 보안 규칙에 프로파일을 할당합니다.

로그 포워딩을 트리거할 각 규칙에 대해 다음 단계를 수행하십시오.

1. 규칙 베이스(예:정책 > 보안 > 사전 규칙)를 선택하고 로그를 포워딩할 방화벽의 디바이스 그룹을 선택한 다음 규칙을 편집합니다.
2. 작업을 선택한 다음 생성한 로그 포워딩 프로파일을 선택합니다.
3. 프로파일 유형을 프로파일 또는 그룹으로 설정한 다음 다음에 대해 로그 생성 및 포워딩을 트리거하는 데 필요한 보안 프로파일 또는 그룹 프로파일을 선택합니다.
   - 위협 로그 - 트래픽이 규칙에 할당된 모든 보안 프로파일과 일치해야 합니다.
   - WildFire 로그 - 트래픽은 규칙에 할당된 WildFire 분석 프로파일과 일치해야 합니다.
4. 트래픽 로그의 경우 세션 시작 시 로그 및/또는 세션 종료 시 로그를 선택합니다.

   세션 시작 시 로깅은 세션 종료 시에만 로깅하는 것보다 더 많은 리소스를 소비합니다. 대부분의 경우 세션 종료 시 로깅만 합니다. 세션 시작 시 로깅 및 세션 종료 시 로깅은 문제 해결, GRE 터널과 같이 수명이 긴 터널 세션(세션 시작 시 로그하지 않으면 ACC에서 이러한 세션을 볼 수 없음)에 대해서만 사용하도록 설정하고, 유효 기간이 긴 세션인 운영 기술/산업 제어 시스템(OT/ICS) 세션에 대한 가시성을 확보하기 위한 경우에만 사용하도록 설정합니다.
5. 규칙을 저장하려면 확인을 클릭합니다.

STEP 5 | 시스템 로그, 구성 로그, User-ID™ 로그 및 HIP 일치 로그의 대상을 구성합니다.

*Panorama*는 방화벽에서 상관 관계 로그를 집계하는 대신 수신한 방화벽 로그를 기반으로 상관 관계 로그를 생성합니다.

1. 디바이스 > 로그 설정을 선택하고 로그를 포워딩할 방화벽의 템플릿을 선택합니다.
2. 방화벽이 포워딩할 각 로그 유형에 대해서는 단계 하나 이상의 일치 목록 프로파일 추가를 참조하십시오.

STEP 6 | (PA-7000 시리즈 방화벽에만 해당) 로그 포워딩을 수행하도록 로그 카드 인터페이스를 구성합니다.

PA-7000 시리즈 NPC(네트워크 처리 카드) 중 하나의 데이터 포트를 로그 카드 인터페이스로 구성하면 방화벽이 자동으로 이 인터페이스를 사용하여 구성한 로깅 대상으로 로그를 포워딩하고 WildFire

 ©2024 Palo Alto Networks, Inc.

분석을 위해 파일을 포워딩하기 시작합니다. 구성한 인터페이스가 로그 포워딩 대상과 WildFire 클라우드, WildFire 어플라이언스 또는 둘 다에 도달할 수 있는지 확인하십시오.

PA-7000 시리즈 방화벽은 이제 *Panorama*에 로그를 포워딩할 수 있으므로 *Panorama*는 더 이상 *PA-7000* 시리즈 방화벽을 로그 수집기로 취급하지 않습니다. *PA-7000* 시리즈 방화벽이 *Panorama*로 로그를 포워딩하도록 구성하지 않은 경우 관리되는 *PA-7000* 시리즈 방화벽이 생성하는 모든 로그는 *Panorama*가 아닌 로컬 방화벽에서만 볼 수 있습니다. *PA-7000* 시리즈 방화벽의 로깅 속도와 볼륨을 처리할 수 있는 로그 포워딩 인프라가 아직 없는 경우 *PAN-OS 8.0.8*부터 *Panorama*를 활성화하여 로그를 모니터링할 때 *PA-7000* 시리즈 방화벽을 직접 쿼리할 수 있습니다. 이 기능을 사용하려면 *Panorama*와 *PA-7000* 시리즈 방화벽이 모두 *PAN-OS 8.0.8* 이상의 버전을 실행해야 합니다. *Panorama CLI*에서

```
> debug reportd send-request-to-7k yes
```

명령을 입력하여 *Panorama*가 *PA-7000* 시리즈 방화벽을 직접 쿼리하도록 합니다.

이 명령을 실행하면 *Panorama* ***Monitor*** 탭에서 관리되는 *PA-7000* 시리즈 방화벽에 대한 로그를 볼 수 있습니다. 또한 모든 관리 디바이스와 마찬가지로 원격 디바이스 데이터를 데이터 소스로 선택하여 *PA-7000* 시리즈 로그 데이터를 포함하는 보고서를 생성할 수도 있습니다. 나중에 *PA-7000* 시리즈 방화벽이 로그를 *Panorama*로 포워딩하도록 설정하기로 결정한 경우 ***### ### send-request-to-7k no*** 명령을 사용하여 먼저 이 옵션을 비활성화해야 합니다.

1. 네트워크 > 인터페이스 > 이더넷을 선택하고 로그를 포워딩할 방화벽의 템플릿을 선택한 다음 인터페이스 추가를 선택합니다.
2. 슬롯 및 인터페이스 이름을 선택합니다.
3. 인터페이스 유형을 로그 카드로 설정합니다.
4. **IP** 주소, 기본 게이트웨이 및 (IPv4에만 해당) 넷마스크를 입력합니다.
5. 고급을 선택한 다음 링크 속도, 링크 이중 및 링크 상태를 지정합니다.

   이러한 필드는 기본적으로 ***auto***로 설정되어 있으며, 방화벽이 연결을 기반으로 값을 자동으로 결정하도록 지정합니다. 그러나 모든 연결에 권장되는 최소 링크 속도는 ***1000****(Mbps)* 입니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 7 | 로그를 수신하도록 Panorama를 구성합니다.

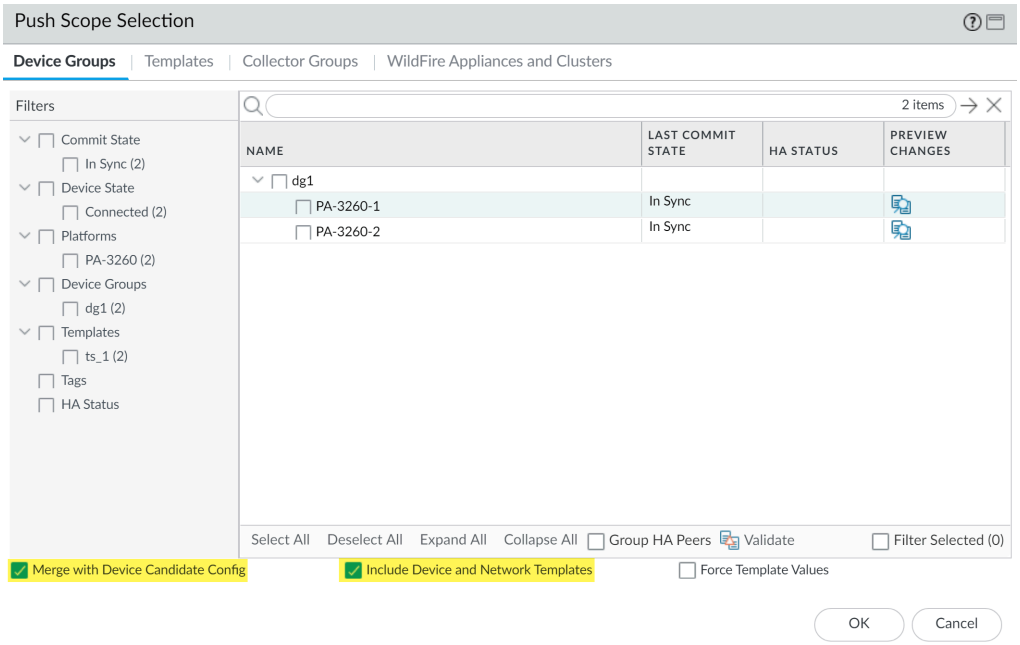
레거시 모드에서 *Panorama* 가상 어플라이언스에 로그를 포워딩하려는 경우 이 단계를 건너뛸 수 있습니다.

1. 로그를 수신할 각 로그 수집기에 대해 관리형 수집기를 구성합니다.
2. 로그 포워딩을 위해 특정 로그 수집기에 방화벽을 할당하도록 수집기 그룹을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 구성 변경 사항을 커밋합니다.

1. 커밋 > 커밋 및 푸시를 선택하고 선택 편집을 선택합니다.
2. 디바이스 후보 구성과 병합 및 디바이스 및 네트워크 템플릿 포함을 선택합니다.



3. 수집기 그룹을 클릭하여 대상 수집기 그룹이 선택되었는지 확인하고 확인을 클릭합니다.
4. Panorama에 변경 사항을 커밋 및 푸시하고 디바이스 그룹, 템플릿 및 수집기 그룹에 변경 사항을 푸시합니다.
5. Panorama로의 로그 포워딩을 확인하여 구성이 성공했는지 확인합니다.

> 방화벽이 *Panorama*에 로그를 보내는 데 사용하는 로그 포워딩 모드를 변경하려면 로그 포워딩 및 버퍼링 기본값을 수정하면 됩니다. 로그 및 보고서에 대한 저장소 할당량 및 만료 기간을 관리할 수도 있습니다.

©2024 Palo Alto Networks, Inc.

외부 대상에 대한 Syslog 포워딩 구성

로그 생성 비율이 높은 배포의 경우 이더넷 인터페이스를 통해 syslog를 포워딩하여 로그 손실을 방지하고 관리 인터페이스의 부하를 줄여 관리 작업을 최적화할 수 있습니다.

이더넷 인터페이스를 사용한 Syslog 포워딩은 Panorama 모드 또는 Log Collector 모드의 Panorama™ 관리 서버에 대해서만 지원됩니다. 또한 Panorama가 Panorama 모드인지 Log Collector 모드인지에 관계없이 단일 인터페이스에서만 syslog 포워딩을 활성화할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | 관리형 수집기 구성.

STEP 3 | 수집기 그룹 구성.

M-시리즈 어플라이언스에서 기본 수집기 그룹은 사전 정의되어 있으며 이미 로컬 로그 수집기를 구성원으로 포함합니다. 그러나 Panorama 가상 어플라이언스에서는 Collector Group을 추가하고 로컬 Log Collector를 구성원으로 추가해야 합니다. 두 구성 모두에서 로그 포워딩을 위해 로그 수집기에 방화벽을 할당해야 합니다.

STEP 4 | Syslog 서버 프로파일을 구성합니다.

1. **Panorama** > 서버 프로파일 > **Syslog** 및 새 syslog 서버 프로파일 추가를 선택합니다.
2. syslog 서버 프로파일의 이름을 입력합니다.
3. 각 syslog 서버에 대해 Panorama 또는 전용 로그 수집기가 연결하는 데 필요한 정보를 추가합니다.
   - 이름 - syslog 서버의 고유 이름입니다.
   - **Syslog** 서버 - syslog 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.
   - 전송 - syslog 서버와의 통신 방법으로 **UDP**, **TCP** 또는 **SSL**을 선택합니다.
   - 포트 - syslog 메시지를 보낼 때 사용할 포트 번호입니다(기본값은 포트 514의 UDP). Panorama 및 전용 로그 수집기에서 동일한 포트 번호를 사용해야 합니다.
   - 형식 - 사용할 syslog 메시지 형식을 선택합니다. **BSD**(기본값) 또는 **IETF**. 전통적으로 **BSD** 형식은 UDP를 사용하고 **IETF** 형식은 TCP 또는 SSL을 사용합니다.
   - 기능 - syslog 서버 구현에서 우선 순위(PRI) 필드를 계산하려면 syslog 표준 값(기본값은 **LOG_USER**)을 선택합니다. PRI 필드를 사용하여 syslog를 관리하는 방법에 매핑되는 값을 선택하십시오.
4. (선택 사항) Panorama 또는 전용 로그 수집기가 보내는 syslog 메시지 형식을 사용자 지정하려면 사용자 지정 로그 형식을 선택합니다. 다양한 로그 유형에 대한 사용자 지정 형식을 만드는 방법에 대한 자세한 내용은 공통 이벤트 형식 구성 가이드를 참조하십시오.
5. 확인을 클릭하여 syslog 서버 프로파일을 저장합니다.

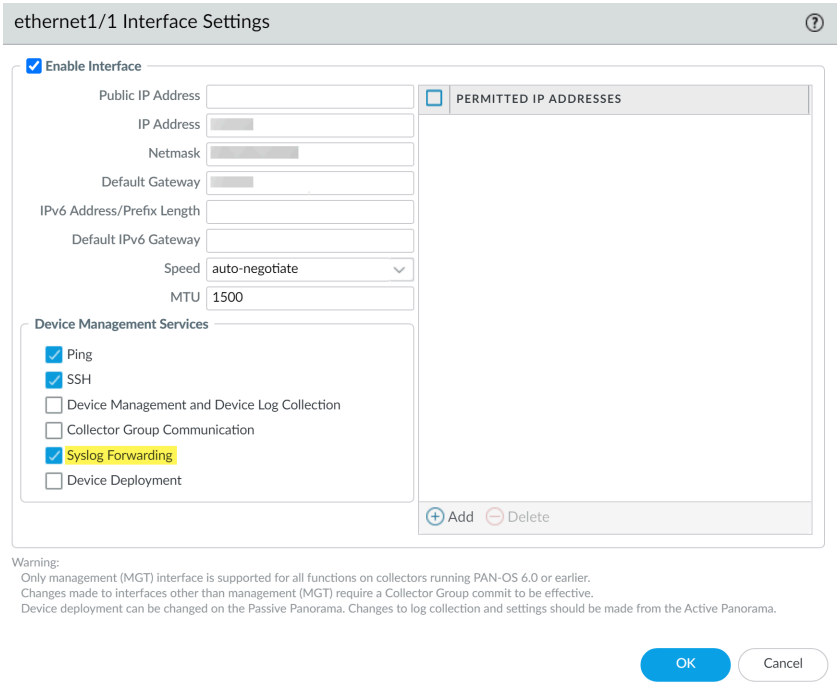
 ©2024 Palo Alto Networks, Inc.

STEP 5 | syslog를 포워딩하기 위한 이더넷 인터페이스를 구성합니다.

기본적으로 syslog 전달은 관리 인터페이스에서 사용하도록 설정되며 한 번에 하나의 인터페이스에서만 지원됩니다.

- Panorama 웹 인터페이스에서 로컬 로그 수집기에서 이더넷 인터페이스를 구성합니다.
  1. **Panorama** > 설정 > 인터페이스를 선택하고 이더넷 인터페이스를 선택합니다.
  2. 인터페이스를 활성화합니다.
  3. 이더넷 인터페이스를 적절하게 구성하십시오.
  4. 디바이스 관리 서비스 섹션에서 **Syslog** 포워딩을 활성화합니다.
  5. 시스템 로그 전달 변경을 확인하려면 예를 선택하십시오.

     로컬 로그 수집기의 단일 이더넷 인터페이스에서만 가능합니다.
  6. 확인을 클릭하여 변경 사항을 저장합니다.
  7. 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

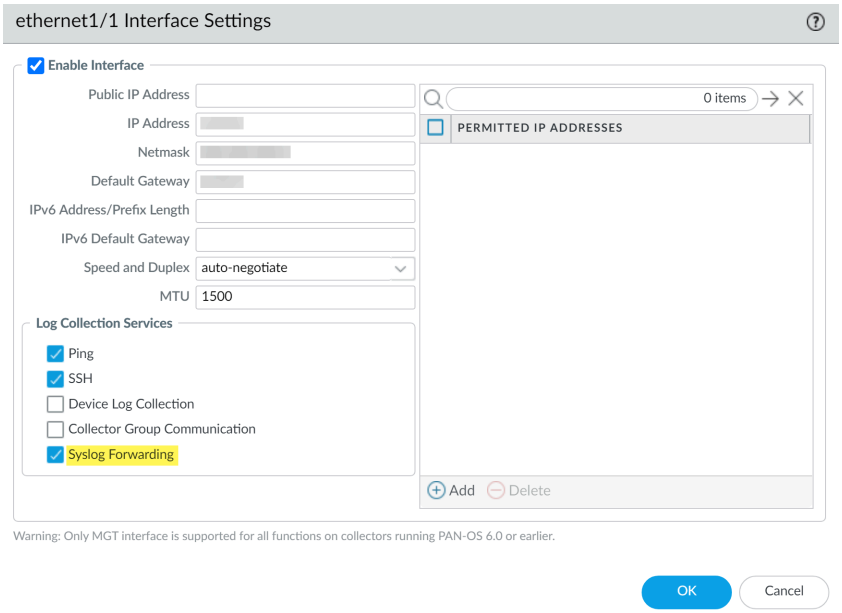


- 전용 로그 수집기에서 이더넷 인터페이스를 구성합니다.
  1. **Panorama** > 관리형 수집기를 선택한 다음 전용 로그 수집기를 선택합니다.
  2. 인터페이스를 활성화합니다.
  3. 이더넷 인터페이스를 적절하게 구성하십시오.
  4. 로그 수집 서비스 섹션에서 **Syslog** 포워딩을 활성화합니다.
  5. 예를 선택하여 syslog 전달 변경을 확인합니다.

     전용 로그 수집기의 단일 이더넷 인터페이스에서만 수행할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

6. 확인을 클릭하여 변경 사항을 저장합니다.
7. 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.



- Panorama CLI에서 로컬 로그 수집기 또는 전용 로그 수집기의 이더넷 인터페이스를 구성합니다.

  CLI에서 이더넷 인터페이스를 통한 syslog 포워딩을 성공적으로 구성하려면 먼저 관리 인터페이스에서 syslog 포워딩을 비활성화한 다음 CLI에서 이더넷 인터페이스에서 syslog 포워딩을 활성화해야 합니다. Panorama는 CLI에서 이더넷 인터페이스에서 syslog 포워딩을 활성화한 관리 인터페이스를 통한 syslog 포워딩을 자동으로 비활성화하지 않으므로 관리 인터페이스와 이더넷 인터페이스 모두에서 활성화하면 관리 인터페이스를 통해 syslog 포워딩이 계속됩니다.

  1. Panorama CLI에 로그인
  2. 관리 인터페이스에서 syslog 포워딩 비활성화:

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system service disable-syslog-forwarding yes
     ```

  3. 이더넷 인터페이스에서 syslog 포워딩 활성화:

     ```
     admin@Panorama> configure
     ```

     ```
     admin@Panorama> set log-collector <Log Collector Serial Number>
      deviceconfig system eth<Interface Number> service disable-
     syslog-forwarding no
     ```

     ```
     admin@Panorama> commit
     ```

 ©2024 Palo Alto Networks, Inc.

4. 구성 변경 사항 커밋:

```
admin@Panorama> run commit-all log-collector-config log-
collector-group <Collector Group name>
```

STEP 6 | Panorama에 대한 로그 포워딩 구성.

STEP 7 | Panorama에서 syslog 서버로 syslog 포워딩을 구성합니다.

©2024 Palo Alto Networks, Inc.

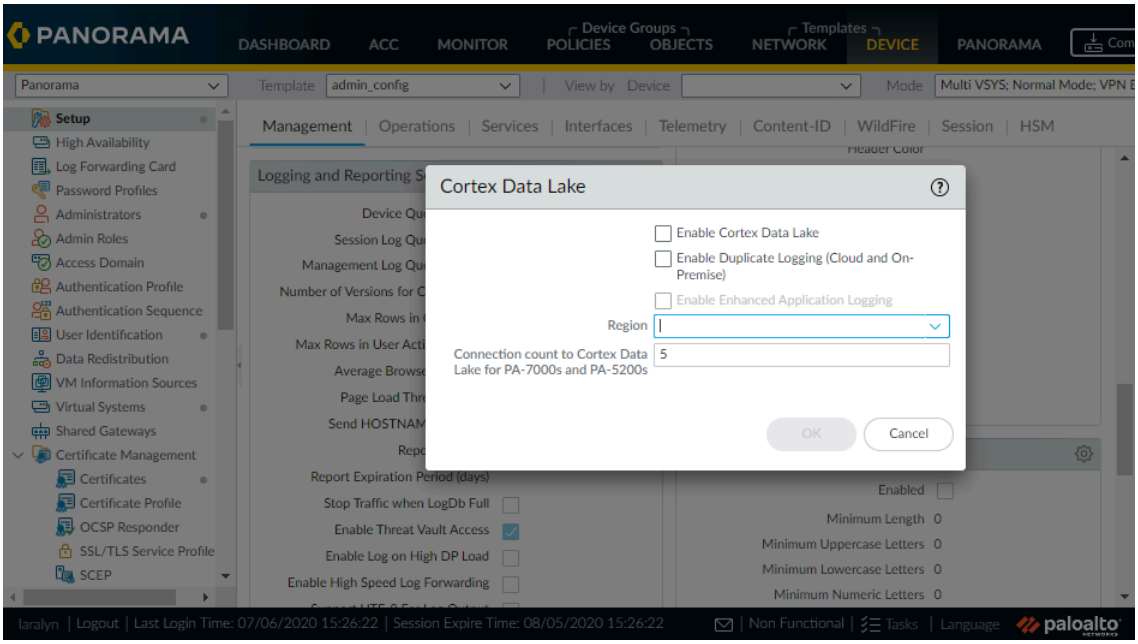
로그를 Strata Logging Service로 포워딩

Strata Logging Service는 Palo Alto Networks의 클라우드 기반 로깅 인프라입니다. Strata Logging Service(이전의 Logging Service)에 로그를 보내도록 관리형 방화벽을 구성하려면 먼저 배포의 로그 볼륨에 대한 라이선스를 구매하고 클라우드 서비스 플러그인을 설치해야 합니다. 이미 온프레미스 로그 수집기가 있는 경우 Strata Logging Service를 사용하여 기존 설정을 보완하고 보강할 수 있습니다.

STEP 1 | Panorama 플러그인 설치.

STEP 2 | Strata Logging Service에 로그를 보내도록 방화벽을 구성합니다.

PAN-OS 8.1 이상의 버전을 실행하는 방화벽의 경우 중복 로깅 활성화(클라우드 및 온프레미스)를 선택할 때 Strata Logging Service와 Panorama 및 온프레미스 로그 수집 설정 모두에 로그를 보내도록 선택할 수 있습니다. 활성화되면 선택한 템플릿에 속한 방화벽이 두 위치에 로그 사본을 저장합니다. 중복 로깅 활성화(클라우드 및 온프레미스) 또는**Strata Logging Service** 활성화 중 하나를 선택할 수 있지만 둘 다 선택할 수는 없습니다.



 ©2024 Palo Alto Networks, Inc.

Panorama로 로그 포워딩 확인

Strata Logging Service 또는 Panorama에 대한 로그 포워딩을 구성한 후 Panorama로 로그 포워딩을 확인하여 구성이 성공했는지 테스트합니다.

로그 수집기에 대한 로그 포워딩을 구성하면 관리 방화벽이 구성된 모든 로그 수집기에 대한 TCP 연결을 엽니다. 이러한 연결은 60초마다 타임아웃되며 방화벽이 로그 수집기에 대한 연결이 끊어졌음을 나타내지 않습니다. 지원되는 이더넷 인터페이스를 통해 로컬 또는 전용 로그 수집기에 대한 로그 포워딩을 구성하면 방화벽이 로그 수집기에 성공적으로 연결할 수 있음에도 불구하고 방화벽 트래픽 로그에 #### 세션이 표시됩니다. 관리 포트를 통해 로그 포워딩을 구성하면 #### 세션을 표시하는 트래픽 로그가 생성되지 않습니다. #### 세션을 표시하는 트래픽 로그는 PA-5200 및 PA-7000 시리즈 방화벽을 제외한 모든 방화벽에서 생성됩니다.

STEP 1 | 방화벽 CLI에 액세스합니다.

STEP 2 | 로그 수집기를 구성한 경우 각 방화벽에 로그 포워딩 기본 설정 목록이 있는지 확인하십시오.

```
> show log-collector preference-list
```

Collector Group에 Log Collector가 하나만 있는 경우 출력은 다음과 같습니다.

```
Forward to all: No Log collector Preference List Serial Number:
 003001000024 IP Address: 10.2.133.48 IPV6 Address: unknown
```

STEP 3 | 각 방화벽이 로그를 포워딩하고 있는지 확인하십시오.

```
> show logging-status
```

성공적인 포워딩의 경우 출력은 로그 포워딩 에이전트가 활성 상태임을 나타냅니다.

- Panorama 가상 어플라이언스의 경우 에이전트는 `Panorama`입니다.
- M 시리즈 어플라이언스의 경우 에이전트는 `LogCollector`입니다.
- Strata Logging Service의 경우 에이전트는 `Log CollectionService`입니다. 그리고

```
'## ## ## ## ####'# ##### <IP_address># #### ####.
```

STEP 4 | 평균 로깅 속도를 확인합니다. 표시된 비율은 지난 5분 동안의 평균 로그/초입니다.

- Log Collectors가 로그를 수신하는 경우 Panorama 웹 인터페이스에 액세스하고 **Panorama** > 관리형 수집기를 선택한 다음 맨 오른쪽 열에서 통계 링크를 클릭합니다.
- 레거시 모드의 Panorama 가상 어플라이언스가 로그를 수신하는 경우 Panorama CLI에 액세스하고 다음 명령을 실행합니다. **`debug log-collector log-collection-stats show arrival-logs`**



이 명령은 M-시리즈 어플라이언스에서도 작동합니다.

©2024 Palo Alto Networks, Inc.

로그 포워딩 및 버퍼링 기본값 수정

방화벽이 Panorama에 로그를 보내는 데 사용하는 로그 포워딩 모드를 정의할 수 있으며, 고가용성(HA) 구성으로 구성된 경우 로그를 수신할 수 있는 Panorama 피어를 지정할 수 있습니다. 이러한 옵션에 액세스하려면 **Panorama** > **Setup** > **Management**를 선택한 다음 로깅 및 보고 설정을 편집한 다음 로그 내보내기 및 보고를 선택합니다.

- 방화벽에서 로그 포워딩 모드를 정의합니다. 방화벽은 버퍼링된 로그 포워딩 모드 또는 라이브 모드 로그 포워딩 모드에서 Panorama(M-시리즈 어플라이언스 및 Panorama 가상 어플라이언스 모두에 해당)로 로그를 포워딩할 수 있습니다.

로깅 옵션	설명
(모범 사례) 디바이스에서 버퍼링된 로그 포워딩 기본: 활성화됨	각 관리 방화벽이 로그를 버퍼링하고 30초 간격으로 Panorama로 로그를 보낼 수 있도록 합니다(사용자 구성 불가). 버퍼링된 로그 포워딩은 방화벽이 Panorama에 대한 연결을 끊을 때 매우 유용합니다. 방화벽은 로그 항목을 로컬 하드 디스크에 버퍼링하고 Panorama에 전송된 마지막 로그 항목을 기록하기 위한 포인터를 유지합니다. 연결이 복원되면 방화벽은 중단된 지점부터 로그 포워딩을 재개합니다. 버퍼링에 사용할 수 있는 디스크 공간은 방화벽 모델의 로그 저장소 할당량과 롤오버 보류 중인 로그의 양에 따라 다릅니다. 방화벽이 오랫동안 연결 해제되어 마지막으로 포워딩된 로그가 롤오버된 경우 로컬 하드 디스크의 모든 로그는 재연결 시 Panorama로 포워딩됩니다. 방화벽의 로컬 하드 디스크에서 사용 가능한 공간이 소모되면 가장 오래된 항목이 삭제되어 새 이벤트를 기록할 수 있습니다.
디바이스에서 라이브 모드 로그 포워딩 이 옵션은 디바이스에서 버퍼링된 로그 포워딩 체크박스가 선택 취소된 경우 활성화됩니다.	라이브 모드에서 관리되는 방화벽은 모든 로그 트랜잭션을 Panorama에 기록하는 동시에 방화벽에 기록합니다.

- 고가용성(HA) 구성에 배포된 레거시 모드의 Panorama 가상 어플라이언스에 대한 로그 포워딩 기본 설정을 정의합니다.
  - 가상 디스크에 로깅할 때 기본 Panorama 피어에서만 로컬 디스크에 로깅을 활성화합니다. 기본적으로 HA 구성의 두 Panorama 피어는 모두 로그를 수신합니다.

    5200 및 *7000* 시리즈 방화벽의 경우 활성 피어만 로그를 수신합니다.

  - NFS(ESXi 서버만 해당)에 로그인할 때 페일오버 후 방화벽이 새로 생성된 로그만 기본으로 승격된 보조 Panorama 피어로 보낼 수 있도록 합니다.

©2024 Palo Alto Networks, Inc.

로깅 옵션	해당	설명
활성 기본 로그만 로컬 디스크에 기록 기본: Disabled	가상 디스크에 로깅하고 HA 구성에 배포되는 레거시 모드의 Panorama 가상 어플라이언스입니다.	로그를 로컬 디스크에 저장하도록 기본 Panorama 피어만 구성할 수 있습니다.
기본으로 변환 시 새 로그만 가져오기 기본: Disabled	NFS(Network File System) 데이터 저장소에 마운트되고 VMware ESXi 서버에서 실행되며 HA 구성으로 배포되는 레거시 모드의 Panorama 가상 어플라이언스	NFS 로깅을 사용하면 고가용성 구성으로 구성된 Panorama 서버 쌍이 있는 경우 기본 Panorama 피어만 NFS 데이터 저장소를 마운트합니다. 따라서 방화벽은 NFS 데이터 저장소에 쓸 수 있는 기본 Panorama 피어로만 로그를 보낼 수 있습니다. HA 페일오버가 발생하면 기본으로 변환 시 새 로그만 가져오기 옵션을 사용하여 관리자는 새로 생성된 로그만 Panorama로 보내도록 관리되는 방화벽을 구성할 수 있습니다. 이 이벤트는 활성-보조 Panorama의 우선순위가 기본으로 승격되고 NFS에 로깅을 시작할 수 있을 때 트리거됩니다. 이 동작은 일반적으로 상당한 시간이 지난 후 Panorama에 대한 연결이 복원될 때 방화벽이 버퍼링된 로그를 대량으로 보내는 것을 방지하기 위해 활성화됩니다.

©2024 Palo Alto Networks, Inc.

Panorama에서 외부 대상으로 로그 포워딩 구성

Panorama를 사용하면 syslog, 이메일, SNMP 트랩 및 HTTP 기반 서비스를 비롯한 외부 서비스에 로그를 포워딩할 수 있습니다. 외부 서비스를 사용하면 중요한 이벤트에 대한 경고를 수신하고, 전용 장기 저장소가 있는 시스템에 모니터링된 정보를 보관하고, 타사 보안 모니터링 도구와 통합할 수 있습니다. 방화벽 로그를 포워딩하는 것 외에도 Panorama 관리 서버 및 로그 수집기가 생성하는 로그를 포워딩할 수 있습니다. 로그를 포워딩하는 Panorama 관리 서버 또는 Log Collector는 로그를 대상(syslog 메시지, 이메일 알림, SNMP 트랩 또는 HTTP 페이로드)에 적합한 형식으로 변환합니다. 전달된 로그의 최대 로그 레코드 크기는 4,096바이트입니다. 로그 레코드 크기가 최대값보다 큰 전달된 로그는 4,096바이트로 잘리고 최대 로그 레코드 크기를 초과하지 않는 로그는 그렇지 않습니다.

로그 전달은 지원되는로그 필드에 대해서만 지원됩니다. 지원되지 않는 로그 필드 또는 의사 필드가 포함된 로그를 전달하면 방화벽이 충돌합니다.

Panorama 관리 서버가 레거시 모드의 *Panorama* 가상 어플라이언스인 경우 로그 수집기를 사용하지 않고 로그를 변환하고 외부 서비스로 포워딩합니다.

방화벽에서 외부 서비스로 직접 로그를 포워딩할 수도 있습니다. 로그 포워딩 옵션을 참조하십시오.

Panorama 5.1 또는 이전 버전을 실행하는 *Panorama* 가상 어플라이언스에서 *CLI*의 SCP(Secure Copy) 명령을 사용하여 전체 로그 데이터베이스를 *SCP* 서버로 내보내고 다른 *Panorama* 가상 어플라이언스로 가져올 수 있습니다. *Panorama 6.0* 이상의 버전을 실행하는 *Panorama* 가상 어플라이언스 및 모든 버전을 실행하는 *M*-시리즈 어플라이언스는 이러한 모델의 로그 데이터베이스가 너무 커서 내보내기 또는 가져오기를 실용적으로 수행할 수 없기 때문에 이러한 옵션을 지원하지 않습니다.

로그를 외부 서비스로 포워딩하려면 먼저 Panorama로 로그를 포워딩하도록 방화벽을 구성하십시오. 그런 다음 Panorama 및 Log Collector가 서비스에 연결하는 방법을 정의하는 서버 프로파일을 구성해야 합니다. 마지막으로 Panorama의 로그 설정과 Collector Groups에 서버 프로파일을 할당합니다.

STEP 1 | Panorama에 로그를 포워딩하도록 방화벽을 구성합니다.

Panorama에 대한 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 로그 정보를 수신할 각 외부 서비스에 대한 서버 프로파일을 구성합니다.

1. **Panorama** > 서버 프로파일을 선택하고 로그 데이터를 수신할 서버 유형을 선택합니다. **SNMP** 트랩, **Syslog**, 이메일 또는 **HTTP**.
2. 서버 프로파일을 구성합니다.
   - SNMP 트랩 서버 프로파일을 구성합니다. SNMP가 Panorama 및 Log Collector에서 작동하는 방식에 대한 자세한 내용은 SNMP 지원을 참조하십시오.
   - Syslog 서버 프로파일을 구성합니다. syslog 서버에 클라이언트 인증이 필요한 경우 **Panorama** > **Certificate** 관리 > 인증서 페이지를 사용하여 SSL을 통한 syslog 통신을 보호하기 위한 인증서를 만드십시오.
   - 이메일 서버 프로파일을 구성합니다.
   - HTTP 서버 프로파일을 구성합니다.

     HTTP 서버로의 로그 포워딩은 낮은 주파수에서의 로그 포워딩을 위해 설계되었으므로 볼륨이 많은 로그 포워딩을 사용하는 배포에는 권장되지 않습니다. 배포 시 포워딩해야 할 로그의 볼륨이 많을 경우 *HTTP* 서버로 포워딩할 때 로그 손실이 발생할 수 있습니다.

STEP 3 | 대상 구성:

- Panorama 관리 서버 및 로그 수집기가 생성하는 로그입니다.
- 방화벽은 레거시 모드의 Panorama 가상 어플라이언스가 수집하는 로그를 기록합니다.

1. **Panorama** > 로그 설정을 선택합니다.
2. 각 로그 유형에 대해 하나 이상의 일치 목록 프로파일을 추가합니다.

   프로파일은 로그 쿼리 필터, 포워딩 대상 및 태깅과 같은 자동 작업을 지정합니다. 각 일치 리스트 프로파일에 대해 다음을 수행합니다.

   1. 프로파일을 식별하려면 이름을 입력합니다.
   2. 로그 유형을 선택합니다.
   3. 필터 드롭다운에서 필터 빌더를 선택합니다. 다음을 지정하고 각 쿼리를 추가합니다.

      커넥터 로직(및/또는)

      로그 속성

      포함 또는 제외 논리를 정의하는 연산자

      일치하는 쿼리의 속성 값
   4. 각 외부 서비스에 대해 구성한 서버 프로파일을 추가합니다.
   5. 확인을 클릭하여 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | Log Collector가 수신하는 방화벽 로그의 대상을 구성합니다.



각 수집기 그룹은 로그를 다른 대상으로 포워딩할 수 있습니다. 로그 수집기가 *Panorama* 관리 서버의 고가용성*(HA)* 쌍에 로컬인 경우 수집기 그룹에 대한 로그 포워딩을 구성하려면 각 *HA* 피어에 로그인해야 합니다.

1. **Panorama** > 수집기 그룹를 선택하고 방화벽 로그를 수신하는 수집기 그룹을 편집합니다.
2. (선택 사항, SNMP 트랩 포워딩만 해당) 모니터링을 선택하고 SNMP 설정을 구성합니다.
3. 필요에 따라 수집기 로그 포워딩 및 구성된 일치 목록 프로파일 추가를 선택합니다.
4. 확인을 클릭하여 수집기 그룹에 대한 변경 사항을 저장합니다.

STEP 5 | (Syslog 포워딩만 해당) syslog 서버에 클라이언트 인증이 필요하고 방화벽이 로그를 전용 로그 수집기로 포워딩하는 경우 SSL을 통한 syslog 통신을 보호하는 인증서를 할당하십시오.

각 전용 로그 수집기에 대해 다음 단계를 수행합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
2. **Secure Syslog**용 인증서를 선택하고 확인을 클릭합니다.

STEP 6 | (SNMP 트랩 포워딩만 해당) SNMP 관리자가 트랩을 해석할 수 있도록 합니다.

지원되는 MIB를 로드하고 필요한 경우 컴파일합니다. 특정 단계의 경우 SNMP 관리자의 설명서를 참조하십시오.

STEP 7 | 구성 변경 사항을 커밋하고 확인합니다.

1. 커밋 > 커밋 및 푸시를 선택하여 Panorama에 변경 사항을 커밋하고 디바이스 그룹, 템플릿 및 수집기 그룹에 변경 사항을 푸시합니다.
2. 외부 서비스가 로그 정보를 수신하고 있는지 확인합니다.
   - 이메일 서버 - 지정된 수신자가 이메일 알림으로 로그를 수신하고 있는지 확인합니다.
   - **Syslog** 서버 - syslog 서버에 대한 설명서를 참조하여 syslog 메시지로 로그를 수신하는지 확인하십시오.
   - **SNMP** 관리자 - SNMP 트랩 서버에 대한 설명서를 참조하여 SNMP 트랩으로 로그를 수신하고 있는지 확인하십시오.
   - **HTTP** 서버 - HTTP 기반 서버가 올바른 페이로드 형식으로 로그를 수신하고 있는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

로그 수집 배포

다음 항목에서는 가장 일반적인 배포에서 로그 수집을 구성하는 방법에 대해 설명합니다. 시작하기 전에 현재 및 미래의 로깅 요구 사항에 따라 Panorama 배포 계획을(를) 수행합니다.

이 주제의 배포에서는 모두 고가용성*(HA)* 구성의 *Panorama*에 대해 설명합니다. *Palo Alto Networks*는 구성 백업의 일부로 저장되지 않은 구성 요소의 자동 복구*(*서버 장애 시*)*를 활성화하기 때문에 *HA*를 권장합니다. *HA* 배포에서 *Panorama* 관리 서버는 활성*/*수동 구성만 지원합니다.

- 전용 로그 수집기로 Panorama 배포
- 로컬 로그 수집기가 있는 Panorama M-시리즈 어플라이언스 배포
- 로컬 로그 수집기로 Panorama 가상 어플라이언스 배포
- 로컬 로그 수집을 사용하여 레거시 모드에서 Panorama 가상 어플라이언스 배포

전용 로그 수집기로 Panorama 배포

다음 그림은 분산 로그 수집 배포의 Panorama를 보여줍니다. 이 예에서 Panorama 관리 서버는 능동/수동 HA(고가용성) 구성으로 배포되는 Panorama 모드의 두 개의 M 시리즈 또는 Panorama 가상 어플라이언스로 구성됩니다. 방화벽은 전용 로그 수집기(로그 수집기 모드의 M 시리즈 또는 Panorama 가상 어플라이언스)로 로그를 보냅니다. 방화벽이 초당 10,000개 이상의 로그를 생성하는 경우 권장되는 구성입니다.

수집기 그룹에 둘 이상의 로그 수집기를 할당하는 경우 요구 사항, 위험 및 권장되는 완화를 이해하려면 다중 로그 수집기가 있는 수집기 그룹에 대한 주의 사항을 참조하십시오.

©2024 Palo Alto Networks, Inc.

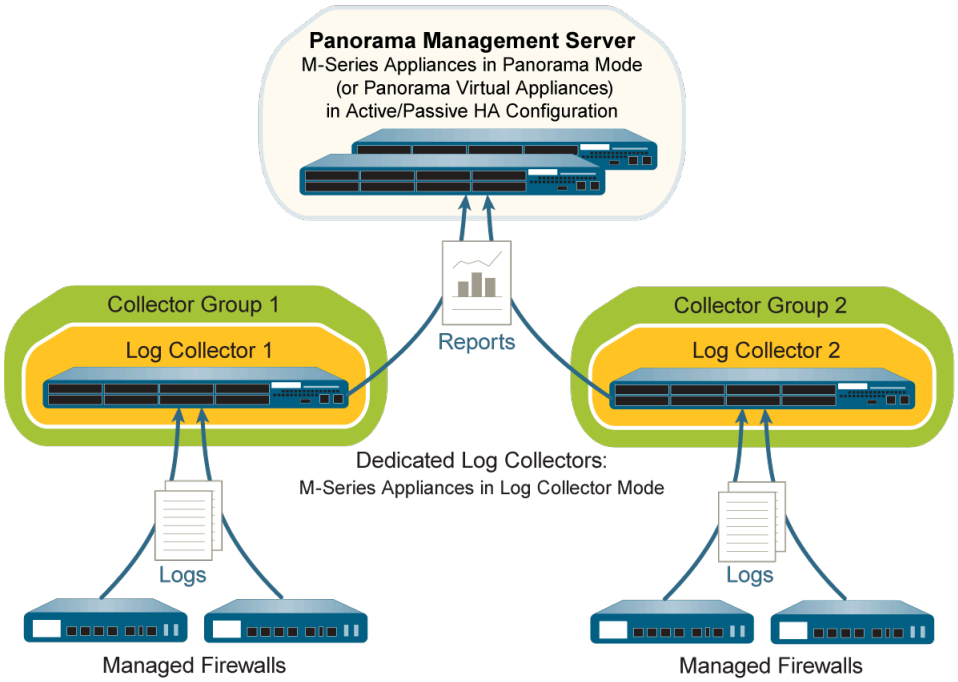


그림 **17:** 수집기 그룹당 단일 전용 로그 수집기

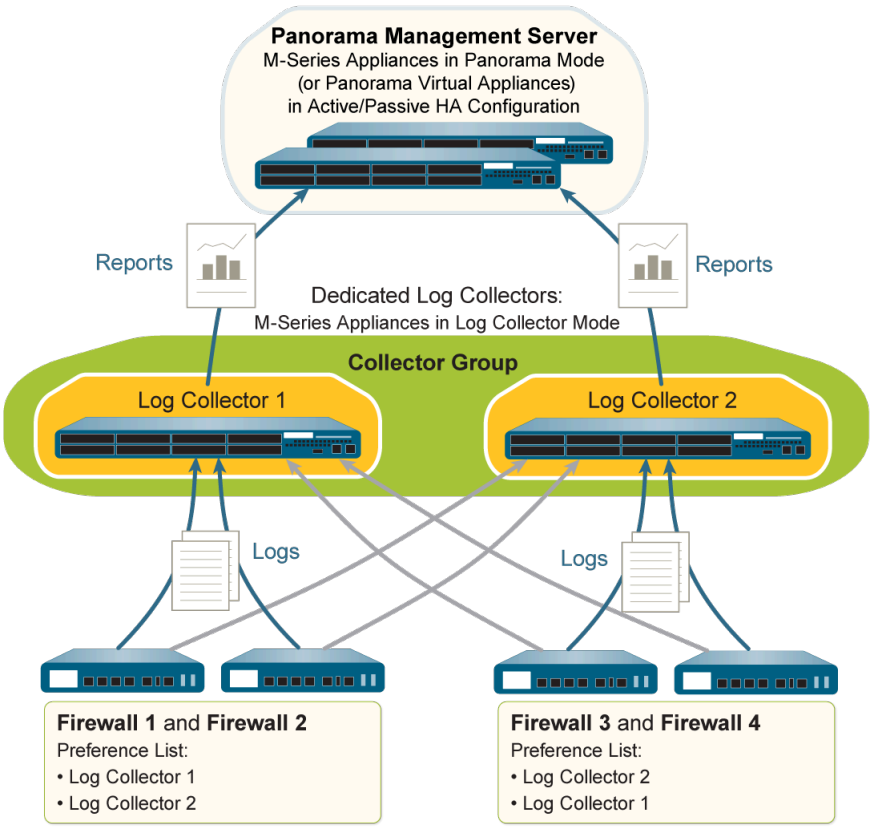


그림 **18:** 수집기 그룹당 여러 개의 전용 로그 수집기

전용 로그 수집기로 Panorama를 배포하려면 다음 단계를 수행하십시오. 이미 수행한 모든 단계(예: 초기 설정)를 건너뜁니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 관리 서버(가상 기기 또는 M-시리즈 기기) 및 전용 로그 수집기의 초기 설정을 수행합니다.

각 M-시리즈 어플라이언스의 경우:

1. M-시리즈 어플라이언스를 랙에 장착합니다. 지침은 M-시리즈 하드웨어 참조 안내서를 참조하십시오.
2. M-시리즈 어플라이언스의 초기 구성 수행.

   *Palo Alto Networks*는 *Panorama*에 대한 관리 액세스를 위해 관리*(MGT)* 인터페이스를 예약하고 별도의 M-시리즈 어플라이언스 인터페이스를 다른 *Panorama* 서비스 전용으로 사용할 것을 권장합니다.
3. 각 어레이를 구성합니다. 이 작업은 RAID 디스크를 로깅에 사용할 수 있도록 하는 데 필요합니다. 선택적으로 디스크를 추가하여 M-시리즈 어플라이언스에서 스토리지를 늘릴 수 있습니다.
4. Panorama를 등록하고 라이선스를 설치합니다.
5. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

각 가상 어플라이언스(있는 경우):

1. Panorama 가상 어플라이언스 설치.
2. Panorama 가상 어플라이언스의 초기 구성 수행.
3. Panorama를 등록하고 라이선스를 설치합니다.
4. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

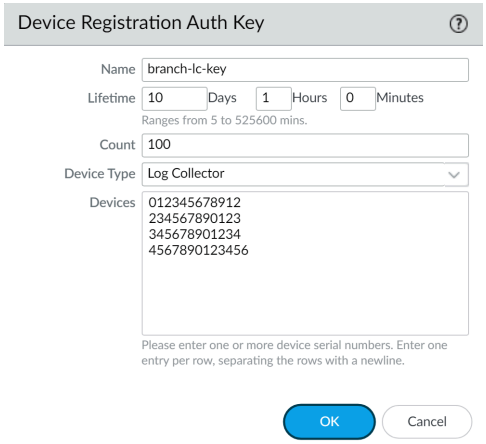
Panorama 관리 서버(가상 어플라이언스 또는 M-시리즈 어플라이언스)의 경우 Panorama에서 HA를 설정해야 합니다.

 ©2024 Palo Alto Networks, Inc.

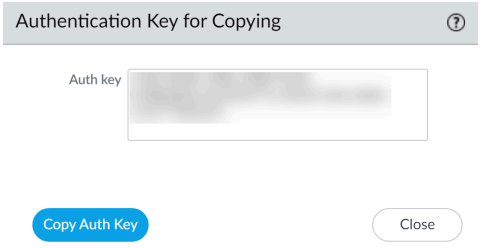
STEP 2 | Panorama 관리 서버에서 디바이스 등록 인증 키를 만들어 전용 로그 수집기를 Panorama 관리에 안전하게 추가합니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
3. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 기간에 대한 키 수명을 지정합니다.
   - 개수 - 인증 키를 사용하여 새 로그 수집기를 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 이 인증 키가 로그 수집기를 인증하는 데만 사용되도록 지정합니다.

     모두를 선택하여 방화벽, 로그 수집기 및 *WildFire* 어플라이언스를 온보딩하는 디바이스 등록 인증 키를 사용할 수 있습니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 로그 수집기를 지정할 하나 이상의 디바이스 일련번호를 입력합니다.
4. 확인을 클릭합니다.



5. 인증 키를 복사하고 닫습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 3 | 전용 로그 수집기가 될 각 Panorama 관리 서버에서 Panorama 모드에서 로그 수집기 모드로 전환합니다.

M-시리즈 또는 *Panorama* 가상 어플라이언스의 모드를 전환하면 기존 로그 데이터가 삭제되고 관리 액세스 설정을 제외한 모든 구성이 삭제됩니다. 전환 후 *M*-시리즈 또는 *Panorama* 가상 어플라이언스는 *CLI* 액세스를 유지하지만 웹 인터페이스 액세스는 잃게 됩니다.

1. 다음 방법 중 하나로 Panorama에 연결합니다.
   - (M-시리즈 기기만 해당) 컴퓨터의 직렬 케이블을 M-시리즈 기기의 콘솔 포트에 연결합니다. 그런 다음 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 초기 구성 중에 Panorama 관리 서버의 MGT 인터페이스에 대해 지정한 IP 주소에 대한 SSH 세션을 엽니다.
2. 메시지가 표시되면 CLI에 로그인합니다. 초기 구성 중에 지정한 기본 관리자 계정과 암호를 사용합니다.
3. 다음 명령을 입력하여 로그 수집기 모드로 전환합니다.

```
> request system system-mode logger
```

4. **Y**를 입력하여 모드 변경을 확인합니다. Panorama 관리 서버가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 Panorama에 다시 연결하여 Panorama 로그인 프롬프트를 확인하십시오.

   CMS *###* 프롬프트가 표시되면 로그 수집기가 재부팅을 완료하지 않았음을 의미합니다. 사용자 이름이나 암호를 입력하지 않고 프롬프트에서 *Enter* 키를 누릅니다.
5. CLI에 다시 로그인합니다.
6. 로그 수집기 모드로의 전환이 성공했는지 확인합니다.

```
> show system info | match system-mode
```

모드 변경이 성공하면 출력이 다음과 같이 표시됩니다.

```
system-mode: logger
```

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 전용 로그 수집기 CLI에서 보안 연결 상태를 재설정합니다.

1. 보안 연결 상태를 재설정합니다.

   이 명령은 관리되는 디바이스 연결을 재설정하고 되돌릴 수 없습니다.

   ```
   admin> request sc3 reset
   ```

2. 관리되는 디바이스에서 관리 서버를 다시 시작합니다.

   ```
   admin> ### ##### ### #### ##-##
   ```

STEP 5 | 전용 로그 수집기에 디바이스 등록 인증 키를 추가합니다.

```
admin> ## # ## <auth-key> ##
```



STEP 6 | 각 Log Collector와 Panorama 관리 서버 간의 연결을 활성화합니다.

이 단계는 로그 수집기에서 디스크 로깅을 활성화하기 전에 필요합니다.

각 로그 수집기의 CLI에서 다음 명령어를 입력합니다. *<IPaddress1>*은(는) 활성 Panorama의 MGT 인터페이스용이고 *<IPaddress2>*은(는) 패시브 Panorama의 MGT 인터페이스용입니다.

```
> configure # set deviceconfig system panorama-server <IPaddress1>
 panorama-server-2 <IPaddress2> # commit # exit
```

STEP 7 | 각 로그 수집기의 일련번호를 기록합니다.

Panorama 관리 서버에서 로그 수집기를 관리 수집기로 추가하려면 일련번호가 필요합니다.

1. 각 로그 수집기의 CLI에서 다음 명령을 입력하여 일련번호를 표시합니다.

   ```
   > show system info | match serial
   ```

2. 일련번호를 기록하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 각 로그 수집기를 관리 수집기로 추가합니다.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 관리형 수집기를 구성합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 관리되는 수집기를 추가합니다.
2. 일반 탭에서 로그 수집기에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
3. **Panorama Server IP** 필드 및 **Panorama Server IP 2** 필드에 활성 및 수동 Panorama HA 피어의 IP 주소 또는 FQDN을 각각 입력합니다. 이 필드는 필수입니다.
4. 인터페이스를 선택한 다음 관리를 클릭한 후 네트워크의 IP 프로토콜을 기반으로 MGT 인터페이스에 대해 다음 필드 세트 중 하나 또는 둘 다를 구성합니다.

   인터페이스에 대해 퍼블릭 ***IP*** 주소를 구성하는 경우 컬렉터 그룹의 로그 수집기는 항상 컬렉터 그룹 내 통신에 퍼블릭 *IP* 주소를 사용합니다. 수집기의 로그 수집기가 프라이빗 *IP* 주소를 사용하여 통신하도록 하려면 퍼블릭 *IP* 주소를 구성하지 마십시오.

   - IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
5. (선택 사항) SNMP 관리자를 사용하여 로그 수집기 통계를 모니터링하려면 **SNMP**를 선택합니다.

   SNMP를 사용하려면 로그 수집기 구성 외에 추가 단계가 필요합니다(SNMP를 사용하여 Panorama 및 로그 수집기 통계 모니터링 참조).
6. 확인을 클릭하여 변경 사항을 저장합니다.
7. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

   이 단계는 로그 수집기에서 디스크 로깅을 활성화하기 전에 필요합니다.
8. **Panorama** > 관리형 수집기 페이지에 추가한 로그 수집기가 나열되는지 확인합니다. 연결됨 열에는 로그 수집기가 Panorama에 연결되었음을 나타내는 확인 표시가 표시됩니다. 페이지에 업데이트된 연결 상태가 표시될 때까지 몇 분 정도 기다려야 할 수 있습니다.

   이 시점에서 구성 상태 열에는 동기화되지 않음이 표시되고 런타임 상태 열에는 연결 끊김이 표시됩니다. 수집기 그룹을 구성하면(9단계) 상태가 동기화 중 및 연결됨으로 변경됩니다.

STEP 9 | 각 로그 수집기에서 로깅 디스크를 활성화합니다.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 다음 단계를 수행합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 Log Collector를 편집합니다.
2. 디스크를 선택한 다음 각 디스크 쌍을 추가하고 확인을 클릭합니다.
3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 10 | (권장) 로그 수집기가 디바이스 로그 수집(방화벽에서 로그 수신) 및 수집기 그룹 통신에 사용할 경우 **Ethernet1**, **Ethernet2**, **Ethernet3**, **Ethernet4** 및 **Ethernet5** 인터페이스를 구성합니다.

기본적으로 로그 수집기는 로그 수집 및 수집기 그룹 통신에 MGT 인터페이스를 사용합니다. 이러한 기능에 다른 인터페이스를 할당하면 관리 트래픽을 위해 MGT 인터페이스를 예약할 수 있습니다. 로그

 ©2024 Palo Alto Networks, Inc.

트래픽이 많은 환경에서는 로그 수집 및 수집기 그룹 통신을 위해 M-500 어플라이언스에서 10Gbps 인터페이스(**Ethernet4** 및 **Ethernet5**)를 사용하는 것을 고려하십시오. 여러 인터페이스에서 로깅 트래픽을 로드 밸런싱하기 위해 여러 인터페이스에서 디바이스 로그 수집을 활성화할 수 있습니다.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 각 로그 수집기에 대해 다음 단계를 수행합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 로그 수집기를 편집한 다음 인터페이스를 선택합니다.
2. 각 인터페이스에 대해 다음 단계를 수행하십시오.
   1. 편집할 인터페이스의 이름을 클릭합니다.
   2. 인터페이스를 활성화하려면 **<interface-name>**을(를) 선택합니다.
   3. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 모두를 완료하십시오.

      IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   4. 인터페이스가 지원하는 디바이스 관리 서비스를 선택합니다.

      디바이스 로그 수집 - 하나 이상의 인터페이스를 할당할 수 있습니다.

      수집기 그룹 통신 - 하나의 인터페이스만 할당할 수 있습니다.
   5. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
3. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.
4. 커밋 > **Panorama**에 커밋를 선택한 다음 Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 11 | 방화벽을 관리 디바이스로 추가하십시오.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 로그 수집기로 로그를 포워딩할 각 방화벽에 대해 이 작업을 수행합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 수집기 그룹을 구성합니다.

각 수집기 그룹에 하나의 로그 수집기가 있는 경우 계속하기 전에 각 수집기 그룹에 대해 이 단계를 반복합니다.

모든 로그 수집기를 하나의 수집기 그룹에 할당하려면 이 단계를 한 번만 수행하십시오.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 수집기 그룹을 구성합니다.

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 추가합니다.
2. 수집기 그룹을 식별할 이름을 입력합니다.
3. 수집기 그룹 구성원 목록에 하나 이상의 로그 수집기를 추가합니다.

   모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.
4. (모범 사례) 단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화합니다. 이 옵션을 사용하려면 각 로그 수집기에 동일한 수의 로깅 디스크가 있어야 합니다.
5. (선택 사항) SNMP를 사용하여 로그 수집기 통계 및 트랩을 모니터링하려면 모니터링을 선택한 다음 설정을 구성합니다.
6. 디바이스 로그 포워딩을 선택한 다음 로그 포워딩 기본 설정 목록을 구성합니다. 이 목록은 어떤 방화벽이 어떤 로그 수집기로 로그를 포워딩하는지 정의합니다. 이 수집기 그룹의 로그 수집기 수에 따라 방화벽을 할당합니다.
   - 단일 - 수집기 그룹당 단일 전용 로그 수집기에 설명된 대로 로그를 해당 로그 수집기로 포워딩할 방화벽을 할당합니다.
   - 다중 - 중복성을 위해 각 방화벽을 두 로그 수집기에 할당합니다. 기본 설정을 구성할 때 수집기 그룹당 여러 개의 전용 로그 수집기에 설명된 대로 Log Collector 1을 방화벽 절반에 대한 첫 번째 우선 순위로 지정하고 Log Collector 2를 다른 절반에 대한 첫 번째 우선 순위로 지정합니다.
7. 확인을 클릭하여 수집기 그룹에 대한 변경 사항을 저장합니다.
8. 커밋 > 커밋 및 푸시를 선택한 다음 Panorama 및 추가한 수집기 그룹에 변경 사항을 커밋 및 푸시합니다.
9. **Panorama** > 관리형 수집기를 선택하여 로그 수집기 구성이 Panorama와 동기화되었는지 확인합니다.

   구성 상태 열은 동기화 중으로 표시되어야 하고 런타임 상태 열은 연결됨으로 표시되어야 합니다.

STEP 13 | 방화벽에서 Panorama로의 로그 포워딩을 구성합니다.

기본 Panorama 관리 서버 피어의 웹 인터페이스를 사용하여 다음을 수행합니다.

1. Panorama에 대한 로그 포워딩을 구성합니다.
2. Panorama로 로그 포워딩 확인.
3. (선택 사항) Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

로컬 로그 수집기가 있는 Panorama M-시리즈 어플라이언스 배포

다음 그림은 중앙 집중식 로그 수집 배포의 Panorama를 보여줍니다. 이 예에서 Panorama 관리 서버는 능동/수동 고가용성(HA) 구성으로 배포되는 Panorama 모드의 M-시리즈 어플라이언스 2개로 구성됩니다. 방화벽은 각 Panorama M-Series 어플라이언스의 사전 정의된(기본값) 로컬 Log Collector로 로그를 보냅니다. 방화벽이 초당 최대 10,000개의 로그를 생성하는 경우 권장되는 배포입니다.

수집기 그룹에 둘 이상의 로그 수집기를 할당하는 경우 요구 사항, 위험 및 권장되는 완화를 이해하려면 다중 로그 수집기가 있는 수집기 그룹에 대한 주의 사항을 참조하십시오.

이 배포를 구현한 후 로깅 속도가 초당 *10,000*개 이상으로 증가하면 *Palo Alto Networks*는 전용 로그 수집기로 Panorama 배포에 설명된 대로 전용 로그 수집기(로그 수집기 모드의 *M*-시리즈 어플라이언스)를 추가할 것을 권장합니다. 이러한 확장을 위해서는 로컬 로그 수집기에서 전용 로그 수집기로 방화벽을 재할당해야 할 수 있습니다.

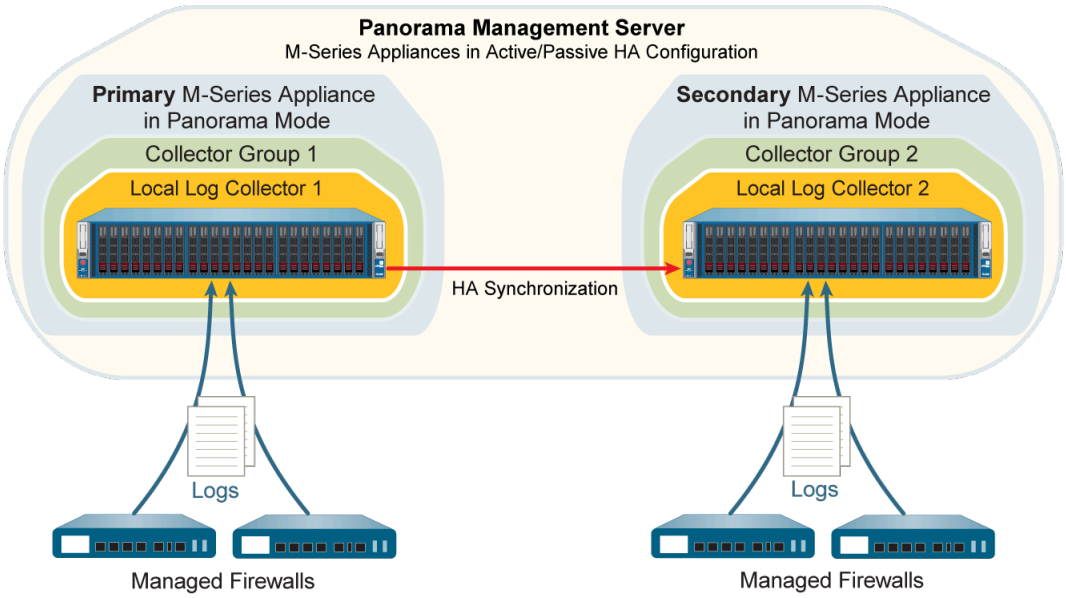


그림 **19:** 수집기 그룹당 단일 로컬 로그 수집기

©2024 Palo Alto Networks, Inc.

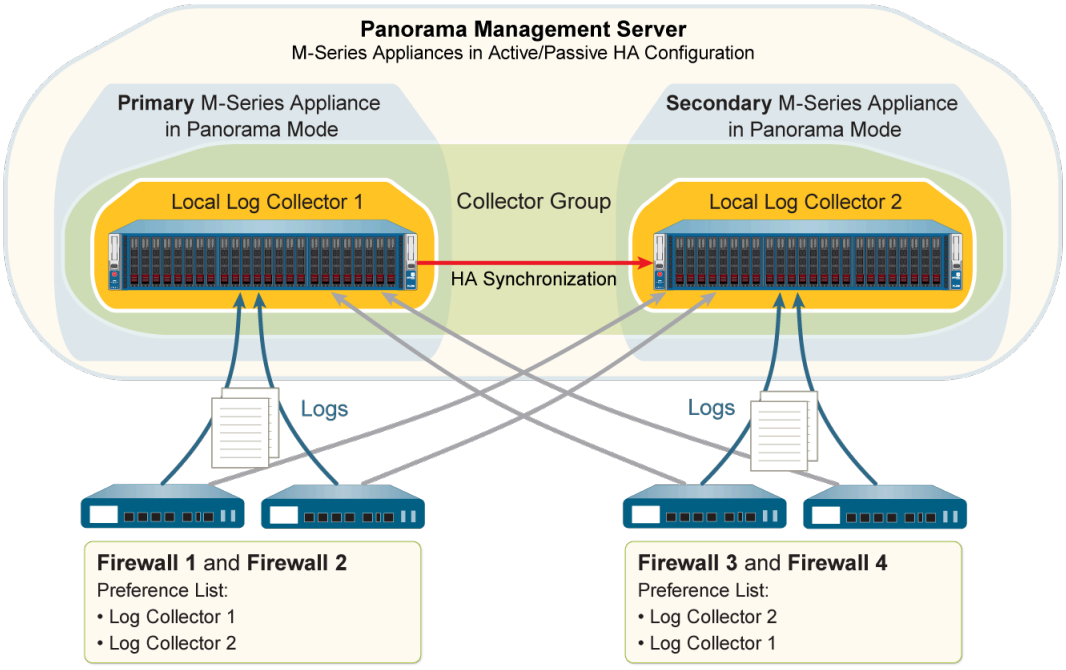


그림 **20:** 수집기 그룹당 여러 로컬 로그 수집기

로컬 로그 수집기로 Panorama를 배포하려면 다음 단계를 수행하십시오. 이미 수행한 모든 단계(예: 초기 설정)를 건너뜁니다.

STEP 1 | 각 M-시리즈 어플라이언스의 초기 설정을 수행합니다.

1. M-시리즈 어플라이언스를 랙에 장착합니다. 지침은 M-시리즈 하드웨어 참조 가이드를 참조하십시오.
2. M-시리즈 어플라이언스의 초기 구성 수행.

   *Palo Alto Networks*는 *Panorama*에 대한 관리 액세스를 위해 관리*(MGT)* 인터페이스를 예약하고 별도의 M-시리즈 어플라이언스 인터페이스를 다른 *Panorama* 서비스 전용으로 사용할 것을 권장합니다.
3. 각 어레이를 구성합니다. 이 작업은 RAID 디스크를 로깅에 사용할 수 있도록 하는 데 필요합니다. 선택적으로 디스크를 추가하여 M-시리즈 어플라이언스에서 스토리지를 늘릴 수 있습니다.
4. Panorama를 등록하고 라이선스를 설치합니다.
5. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.
6. Panorama에서 HA 설정.

©2024 Palo Alto Networks, Inc.

STEP 2 | 로그 수집을 위해 Panorama를 준비하려면 다음 단계를 수행하십시오.

1. 다음 방법 중 하나로 기본 Panorama에 연결합니다.
   - 컴퓨터의 직렬 케이블을 기본 Panorama의 콘솔 포트에 연결합니다. 그런 다음 터미널 에뮬레이션 소프트웨어(9600-8-N-1)를 사용하여 연결합니다.
   - PuTTY와 같은 터미널 에뮬레이션 소프트웨어를 사용하여 초기 구성 중에 기본 Panorama의 MGT 인터페이스에 대해 지정한 IP 주소에 대한 SSH 세션을 엽니다.
2. 메시지가 표시되면 CLI에 로그인합니다. 초기 구성 중에 지정한 기본 관리자 계정과 암호를 사용합니다.
3. 다음 명령을 입력하여 기본 Panorama가 보조 Panorama에 연결할 수 있도록 합니다. 여기서 <*IPaddress2*>은(는) 보조 Panorama의 MGT 인터페이스를 나타냅니다.

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress2> # commit
   ```

4. 보조 Panorama의 CLI에 로그인합니다.
5. 다음 명령을 입력하여 기본 Panorama에 연결하도록 보조 Panorama를 활성화합니다. 여기서 <*IPaddress1*>은(는) 기본 Panorama의 MGT 인터페이스를 나타냅니다.

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress1> # commit # exit
   ```

6. 보조 Panorama의 CLI에서 다음 명령을 입력하여 일련번호를 표시한 후 기록합니다.

   ```
   > show system info | match serial
   ```

   보조 Panorama의 Log Collector를 관리 수집기로 기본 Panorama에 추가하려면 일련번호가 필요합니다.

STEP 3 | 기본 Panorama에 로컬인 로그 수집기를 편집합니다.

기본 Panorama의 웹 인터페이스를 사용하여 다음 단계를 수행합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 기본 (로컬) 로그 수집기를 선택합니다.
2. 디스크를 선택한 다음 각 로깅 디스크 쌍을 추가합니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 보조 Panorama에 로컬인 로그 수집기를 구성합니다.

*Panorama*는 이 *Log Collector*가 기본 *Panorama*에 로컬이 아니기 때문에 원격으로 취급합니다. 따라서 기본 *Panorama*에 수동으로 추가해야 합니다.

기본 Panorama의 웹 인터페이스를 사용하여 관리형 수집기 구성:

1. **Panorama** > 관리형 수집기를 선택한 다음 로그 수집기를 추가합니다.
2. 보조 Panorama의 로그 수집기에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
3. **Panorama Server IP** 필드 및 **Panorama Server IP 2** 필드에 기본 및 보조 Panorama HA 피어의 IP 주소 또는 FQDN을 각각 입력합니다.

   이 두 필드는 모두 필수입니다.
4. 인터페이스를 선택한 다음 로그 수집기가 사용할 각 인터페이스를 구성합니다. 관리 인터페이스가 필요합니다. 각 인터페이스에 대해 다음 단계를 수행하십시오.
   1. 인터페이스 이름을 클릭합니다.
   2. 네트워크의 IP 프로토콜을 기반으로 다음 필드 세트 중 하나 또는 둘 다를 구성하십시오.

      IPv4 - **IP** 주소, 넷마스크 및 기본 게이트웨이

      IPv6 - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
   3. (관리 인터페이스만 해당) **SNMP** 관리자를 사용하여 Log Collector 통계를 모니터링하려면 SNMP를 선택하십시오.

      SNMP를 사용하려면 로그 수집기 구성 외에 추가 단계가 필요합니다(SNMP를 사용하여 Panorama 및 로그 수집기 통계 모니터링 참조).
   4. 확인을 클릭하여 인터페이스에 대한 변경 사항을 저장합니다.
5. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.
6. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

   이 단계는 로깅 디스크를 활성화하기 전에 필요합니다.
7. 이름을 클릭하여 로그 수집기를 편집합니다.
8. 디스크를 선택한 다음 각 RAID 디스크 쌍을 추가하고 확인을 클릭합니다.
9. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 5 | 방화벽을 관리 디바이스로 추가하십시오.

기본 Panorama의 웹 인터페이스를 사용하여 로그 수집기로 로그를 포워딩할 각 방화벽에 대해 이 작업을 수행합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 기본 Panorama에 사전 정의된 기본 수집기 그룹을 편집합니다.

기본 Panorama의 웹 인터페이스를 사용하여 수집기 그룹 구성:

1. **Panorama** > 수집기 그룹을 선택한 다음 기본 수집기 그룹을 편집합니다.
2. 단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 보조 Panorama의 로컬 로그 수집기를 수집기 그룹 구성원 목록에 추가합니다. 기본적으로 목록에는 기본 수집기 그룹에 미리 할당되어 있기 때문에 기본 Panorama의 로컬 로그 수집기가 표시됩니다.

   모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.
3. (모범 사례) 단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화합니다. 이 옵션을 사용하려면 각 로그 수집기에 동일한 수의 로깅 디스크가 있어야 합니다.
4. (선택 사항) SNMP를 사용하여 로그 수집기 통계 및 트랩을 모니터링하려면 모니터링을 선택한 다음 설정을 구성합니다.
5. 디바이스 로그 포워딩을 선택한 다음 로그 포워딩 기본 설정 목록을 구성합니다. 이 목록은 어떤 방화벽이 어떤 로그 수집기로 로그를 포워딩하는지 정의합니다. 이 수집기 그룹의 로그 수집기 수에 따라 방화벽을 할당합니다.
   - 단일 - 수집기 그룹당 단일 로컬 로그 수집기에 설명된 대로 기본 Panorama의 로컬 로그 수집기로 로그를 포워딩할 방화벽을 할당합니다.
   - 다중 - 중복성을 위해 각 방화벽을 두 로그 수집기에 할당합니다. 기본 설정을 구성할 때 수집기 그룹당 다중 로컬 로그 수집기에 설명된 대로 Log Collector 1을 방화벽 절반에 대한 첫 번째 우선 순위로 지정하고 Log Collector 2를 다른 절반에 대한 첫 번째 우선 순위로 지정합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 7 | 보조 Panorama의 로그 수집기를 포함하는 수집기 그룹을 구성합니다.

각 수집기 그룹에 로그 수집기가 하나만 있는 경우 필요합니다.

기본 Panorama의 웹 인터페이스를 사용하여 수집기 그룹 구성:

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 추가합니다.
2. 수집기 그룹을 식별할 이름을 입력합니다.
3. 수집기 그룹 멤버 목록에 보조 Panorama의 로컬 로그 수집기를 추가합니다.
4. (선택 사항) SNMP 관리자를 사용하여 로그 수집기 통계 및 트랩을 모니터링하려면 모니터링을 선택한 다음 설정을 구성합니다.
5. 디바이스 로그 포워딩을 선택한 다음 로그 포워딩 기본 설정 목록에 항목 추가:
   1. 디바이스 목록을 수정하고 보조 Panorama의 로컬 로그 수집기로 로그를 포워딩할 방화벽을 선택한 다음(수집기 그룹당 단일 로컬 로그 수집기 참조) 확인을 클릭합니다.
   2. 보조 Panorama의 로컬 로그 수집기를 수집기 목록에 추가하고 확인을 클릭합니다.
6. 확인을 클릭하여 변경 사항을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | Panorama 구성 및 수집기 그룹에 대한 변경 사항을 커밋하고 푸시합니다.

기본 Panorama의 웹 인터페이스에서 커밋 > 커밋 및 푸시를 선택한 다음, Panorama 및 추가한 수집기 그룹에 대한 변경 사항 커밋 및 푸시를 선택합니다.

STEP 9 | 보조 Panorama가 활성화되도록 수동으로 페일오버합니다.

기본 Panorama의 웹 인터페이스를 사용하여 다음 단계를 수행합니다.

1. **Panorama** > 고가용성을 선택합니다.
2. 작동 명령 섹션에서 로컬 **Panorama** 일시 중지를 클릭합니다.

STEP 10 | 보조 Panorama에서 기본 Panorama에 로컬인 로그 수집기의 네트워크 설정을 구성합니다.

보조 Panorama의 웹 인터페이스를 사용하여 다음 단계를 수행합니다.

1. Panorama 웹 인터페이스에서 **Panorama** > 관리형 수집기를 선택한 다음 기본 Panorama에 로컬인 로그 수집기를 선택합니다.
2. **Panorama Server IP** 필드 및 **Panorama Server IP 2** 필드에 기본 및 보조 Panorama HA 피어의 IP 주소 또는 FQDN을 각각 입력합니다.

   이 두 필드는 모두 필수입니다.
3. 인터페이스를 선택한 다음 관리를 클릭하고 기본 Panorama의 MGT 인터페이스 값으로 다음 필드 세트(네트워크의 IP 프로토콜 기반) 중 하나 또는 둘 다를 완료합니다.
   - **IPv4** - **IP** 주소, 넷마스크 및 기본 게이트웨이
   - **IPv6** - **IPv6** 주소/접두사 길이 및 기본 **IPv6** 게이트웨이
4. 확인을 클릭하여 변경 사항을 저장합니다.
5. 커밋 > 커밋 및 푸시를 선택한 다음, Panorama 및 추가한 수집기 그룹에 대한 변경 사항 커밋 및 푸시를 선택합니다.

STEP 11 | 기본 Panorama가 활성화되도록 수동으로 장애를 복구합니다.

보조 Panorama의 웹 인터페이스를 사용하여 다음 단계를 수행합니다.

1. **Panorama** > 고가용성을 선택합니다.
2. 작동 명령 섹션에서 로컬 **Panorama** 일시 중지를 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 방화벽에서 Panorama로의 로그 포워딩을 구성합니다.

기본 Panorama의 웹 인터페이스를 사용하여 다음을 수행합니다.

1. Panorama에 대한 로그 포워딩을 구성합니다.
2. Panorama로 로그 포워딩 확인.
3. (선택 사항) Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.



각 *Panorama HA* 피어에 별도의 외부 서버 프로파일을 할당할 수 있습니다. 예를 들어, 각 피어가 로그를 다른 *syslog* 서버로 포워딩하도록 할 수 있습니다. 각 *Panorama* 피어가 다른 외부 서비스로 로그를 포워딩하도록 하려면 각 피어의 웹 인터페이스에 로그인하고 ***Panorama*** > ***Collector Groups***를 선택한 다음 *Collector Group*을 선택한 다음 ***Collector Log Forwarding***을 선택한 다음 서버 프로파일을 할당하고 확인을 클릭합니다.

로컬 로그 수집기로 Panorama 가상 어플라이언스 배포

Panorama 모드의 Panorama 가상 어플라이언스에서 로컬로 실행되는 Log Collector에 로그를 보내도록 방화벽을 구성할 수 있습니다. 고가용성(HA) 구성에서 각 Panorama HA 피어는 로컬 로그 수집기를 가질 수 있습니다. 다음 그림과 같이 HA 피어의 로컬 로그 수집기를 동일한 수집기 그룹 또는 별도의 수집기 그룹에 할당할 수 있습니다. VMware 가상 인프라에서 로컬 로그 수집기가 있는 Panorama 가상 어플라이언스를 배포할 때 지원되는 초당 로그를 검토하려면 Panorama 가상 어플라이언스의 전제 조건 설정을(를) 참조하십시오.



수집기 그룹에 둘 이상의 로그 수집기를 할당하는 경우 요구 사항, 위험 및 권장되는 완화를 이해하려면 다중 로그 수집기가 있는 수집기 그룹에 대한 주의 사항을 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

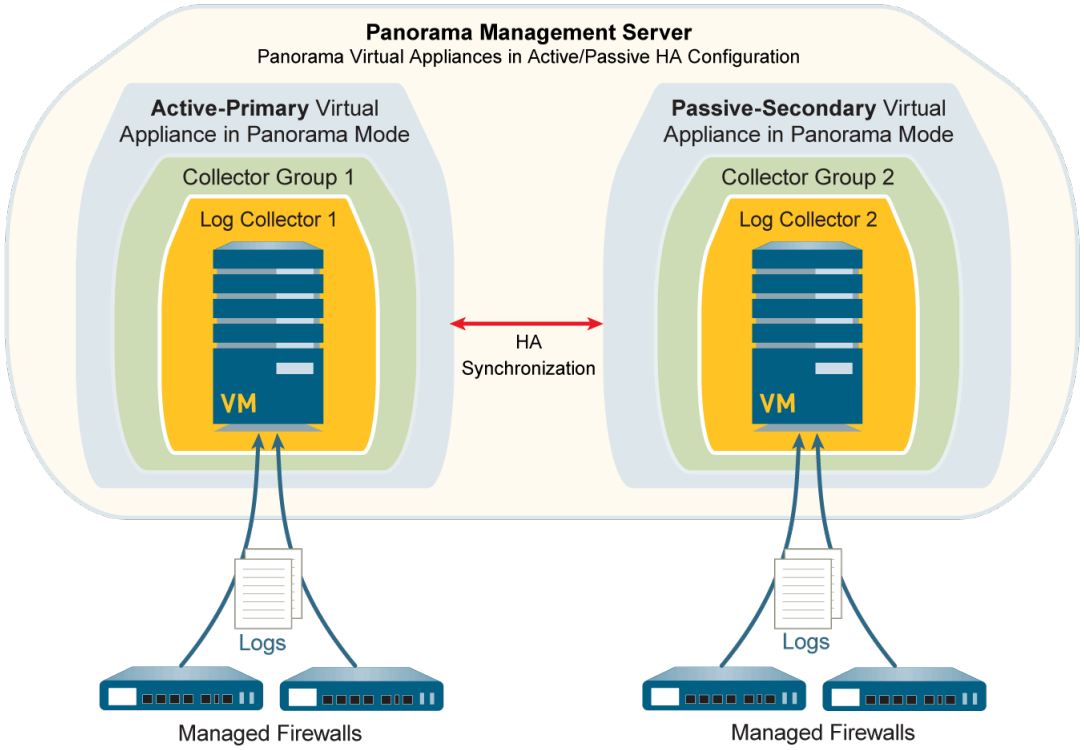


그림 **21:** 수집기 그룹당 단일 로그 수집기

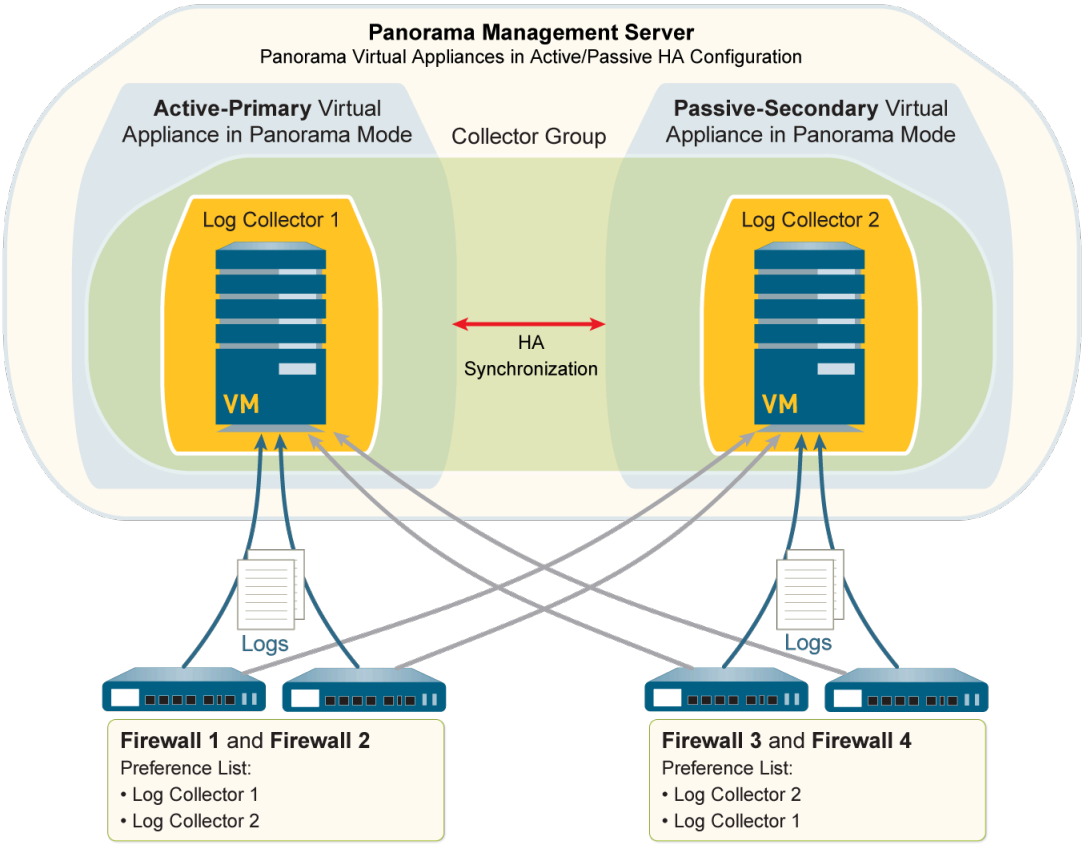


그림 **22:** 수집기 그룹당 여러 로그 수집기

©2024 Palo Alto Networks, Inc.

로컬 로그 수집기로 Panorama를 배포하려면 다음 단계를 수행하십시오. 이미 수행한 단계(예: 초기 설정)를 건너뜁니다.

STEP 1 | 각 Panorama 가상 어플라이언스의 초기 설정을 수행합니다.

1. Panorama 가상 어플라이언스 설치. 가상 어플라이언스가 Panorama 모드에서 시작되도록 하려면 다음 리소스를 구성해야 합니다.
   - 정확히 81GB의 스토리지가 있는 시스템 디스크.
   - Panorama가 수신하고 저장할 로그의 양에 충분한 CPU 및 메모리.
   - 2~24TB의 스토리지가 있는 가상 로깅 디스크.

   *Panorama*는 자동으로 새 디스크를 *2TB* 파티션으로 나누고 각 파티션은 별도의 가상 디스크로 작동합니다.
2. Panorama 가상 어플라이언스의 초기 구성 수행.
3. Panorama를 등록하고 라이선스를 설치합니다.
4. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 2 | HA 구성에서 Panorama 가상 어플라이언스를 설정합니다.

1. Panorama에서 HA 설정.
2. Panorama HA 페일오버 테스트.

STEP 3 | 기본 Panorama에 로컬인 로그 수집기를 추가합니다.

기본 Panorama에서:

1. Panorama 일련번호를 기록합니다.
   1. Panorama 웹 인터페이스에 액세스합니다.
   2. 대시보드를 선택한 다음 일반 정보 섹션에 일련번호를 기록합니다.
2. 로그 수집기를 관리 수집기로 추가합니다.
   1. **Panorama** > 관리형 수집기를 선택한 다음 새 로그 수집기를 추가합니다.
   2. 일반 설정에서 Panorama용으로 기록한 일련번호(**Collector S/N**)를 입력합니다.
   3. 확인을 클릭하여 변경 사항을 저장합니다.
   4. 커밋 > **Panorama**에 커밋을 선택합니다.

      이 단계는 가상 로깅 디스크를 추가하기 전에 필요합니다.
3. 가상 로깅 디스크를 추가합니다.
   1. **Panorama** > 관리형 수집기를 선택한 다음 이름을 클릭하여 Log Collector를 편집합니다.

      Log Collector 이름은 기본 Panorama의 호스트 이름과 동일한 값을 갖습니다.
   2. 디스크를 선택한 다음 가상 로깅 디스크를 추가합니다.
   3. 확인을 클릭하여 변경 사항을 저장합니다.
   4. 커밋 > **Panorama**에 커밋을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 보조 Panorama에 로컬인 로그 수집기를 추가합니다.

*Panorama*는 이 *Log Collector*를 기본 *Panorama*에서 로컬로 실행하지 않기 때문에 원격으로 취급합니다.

1. 보조 Panorama의 일련번호를 기록합니다.
   1. 보조 Panorama의 웹 인터페이스에 액세스합니다.
   2. 대시보드를 선택한 다음 일반 정보 섹션에 일련번호를 기록합니다.
2. 기본 Panorama의 웹 인터페이스에 액세스합니다.
3. **Panorama** > 관리형 수집기를 선택한 다음 로그 수집기를 추가합니다.
4. 일반 설정에서 보조 Panorama에 대해 기록한 일련번호(수집기 **S/N**)를 입력합니다.
5. **Panorama Server IP** 필드 및 **Panorama Server IP 2** 필드에 기본 및 보조 Panorama HA 피어의 IP 주소 또는 FQDN을 각각 입력합니다.

   이 두 필드는 모두 필수입니다.
6. 확인을 클릭하여 변경 사항을 로그 수집기에 저장합니다.
7. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

   이 단계는 가상 로깅 디스크를 추가하기 전에 필요합니다.
8. 이름을 클릭하여 로그 수집기를 편집합니다.

   Log Collector 이름은 보조 Panorama의 호스트 이름과 동일한 값을 갖습니다.
9. 디스크를 선택한 다음 가상 로깅 디스크를 추가하고 확인을 클릭합니다.
10. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

STEP 5 | 방화벽을 관리 디바이스로 추가하십시오.

기본 Panorama를 사용하여 로그 수집기로 로그를 포워딩할 각 방화벽에 대해 이 작업을 수행합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 수집기 그룹을 구성합니다.

두 로그 수집기를 동일한 수집기 그룹에 할당하려면 이 단계를 한 번 수행하십시오. 그렇지 않으면 각 로그 수집기에 대해 수집기 그룹을 구성합니다.

기본 Panorama에서:

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 추가합니다.
2. 하나 또는 두 개의 로그 수집기를 수집기 그룹 구성원으로 추가합니다.

   모든 단일 수집기 그룹에서 모든 로그 수집기는 동일한 *Panorama* 모델인 모든 *M-700* 기기, 모든 *M-600* 기기, 모든 *M-500* 기기, 모든 *M-300* 기기, 모든 *M-200* 기기 또는 모든 *Panorama* 가상 어플라이언스에서 실행되어야 합니다.
3. (모범 사례) 단일 수집기 그룹에 여러 로그 수집기를 추가하는 경우 수집기 간에 로그 중복성을 활성화합니다. 이 옵션을 사용하려면 각 로그 수집기에 동일한 수의 가상 로깅 디스크가 있어야 합니다.

   중복성을 활성화하면 수집기 그룹에서 로그 및 로그 처리 트래픽 양이 두 배로 증가합니다. 필요한 경우 Panorama 가상 어플라이언스에서 로그 스토리지 용량을 확장합니다.
4. 디바이스 로그 포워딩을 선택한 다음 로그 포워딩 기본 설정 목록을 구성합니다. 이 목록은 어떤 방화벽이 어떤 로그 수집기로 로그를 포워딩하는지 정의합니다. 이 수집기 그룹의 로그 수집기 수에 따라 방화벽을 할당합니다.
   - 단일 - 수집기 그룹당 단일 로그 수집기에 설명된 대로 기본 Panorama에 로컬인 로그 수집기로 로그를 포워딩할 방화벽을 할당합니다.
   - 다중 - 중복성을 위해 각 방화벽을 두 로그 수집기에 할당합니다. 기본 설정 목록을 구성할 때 수집기 그룹당 다중 로그 수집기에 설명된 대로 Log Collector 1을 방화벽 절반의 첫 번째 우선 순위로 지정하고 Log Collector 2를 다른 절반의 첫 번째 우선 순위로 지정합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.
6. 커밋 > 커밋 및 푸시를 선택한 다음, Panorama 및 추가한 수집기 그룹에 대한 변경 사항 커밋 및 푸시를 선택합니다.

STEP 7 | 보조 Panorama가 활성화되도록 기본 Panorama에서 페일오버를 트리거합니다.

기본 Panorama에서:

1. **Panorama** > 고가용성을 선택합니다.
2. 작동 명령 섹션에서 로컬 **Panorama** 일시 중지를 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 보조 Panorama에서 기본 Panorama에 로컬인 로그 수집기로의 연결을 구성합니다.

보조 Panorama에서:

1. Panorama 웹 인터페이스에서 **Panorama** > 관리형 수집기를 선택한 다음 기본 Panorama에 로컬인 로그 수집기를 선택합니다.
2. **Panorama Server IP** 필드 및 **Panorama Server IP 2** 필드에 기본 및 보조 Panorama HA 피어의 IP 주소 또는 FQDN을 각각 입력합니다.

   이 두 필드는 모두 필수입니다.
3. 확인을 클릭하여 변경 사항을 저장합니다.
4. 커밋 > 커밋 및 푸시를 선택한 다음 Panorama 및 수집기 그룹에 대한 변경 사항 커밋 및 푸시를 선택합니다.

STEP 9 | 기본 Panorama에서 HA 기능을 복원합니다.

1. 기본 Panorama의 Panorama 웹 인터페이스에 로그인합니다.
2. **Panorama** > 고가용성을 선택합니다.
3. 고가용성을 위해 로컬 **Panorama**가 작동하도록 합니다.

STEP 10 | 기본 Panorama가 활성화되도록 보조 Panorama에서 장애 복구를 트리거합니다.

보조 Panorama에서:

1. **Panorama** > 고가용성을 선택합니다.
2. 작동 명령 섹션에서 로컬 **Panorama** 일시 중지를 클릭합니다.
3. HA 기능을 보조 Panorama로 복원하기 위해 고가용성을 위해 로컬 **Panorama**가 작동하도록 합니다.
4. 대시보드에서 고가용성 위젯에서 보조 Panorama가 ##-##인지 확인합니다.
5. 기본 Panorama의 Panorama 웹 인터페이스에 로그인하고 대시보드에서 기본 Panorama가 ## ##인지 고가용성 위젯에서 확인합니다.

STEP 11 | 방화벽에서 Panorama로의 로그 포워딩을 구성합니다.

기본 Panorama에서:

1. 방화벽에서 Panorama로의 로그 포워딩을 구성합니다.
2. Panorama로 로그 포워딩 확인.

로컬 로그 수집을 사용하여 레거시 모드에서 Panorama 가상 어플라이언스 배포

다음 그림은 중앙 집중식 로그 수집 배포의 Panorama를 보여줍니다. 이 예에서 Panorama 관리 서버는 활성/수동 HA(고가용성) 구성에 배포된 레거시 모드의 두 개의 Panorama 가상 어플라이언스로 구성됩니다. 이 구성은 Panorama가 초당 최대 10,000개의 로그를 처리하는 VMware 가상 인프라 내 방화벽 관리에 적합합니다. 방화벽은 NFS 데이터 저장소(ESXi 서버만 해당) 또는 Panorama 관리 서버의 가상 디스크로 로그를 보냅니다. 기본적으로 활성 피어와 수동 피어 모두 로그를 수신하지만 활성 피어만 수신하도록 로그 포워딩 및 버퍼링 기본값을 수정할 수 있습니다. 5200 및 7000 시리즈 방화벽의 경우 활성 피어만 로그를 수신합니다. 기본적으로 레거시 모드의 Panorama 가상 어플라이언스는 내부 디스크 파티션에서 로그

 ©2024 Palo Alto Networks, Inc.

저장을 위해 약 11GB를 사용하지만 필요한 경우 Panorama 가상 어플라이언스에서 로그 저장소 용량을 확장할 수 있습니다.

로깅 속도가 초당 *10,000*개 이상의 로그로 증가하는 경우 전용 로그 수집기로 Panorama 배포를 권장합니다.

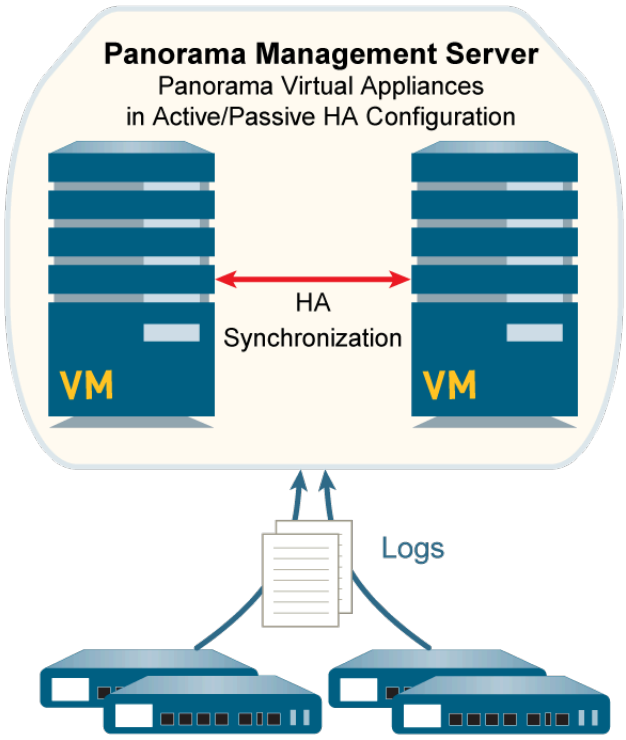


그림 **23:** 로컬 로그 수집이 있는 레거시 모드의 **Panorama** 가상 어플라이언스

로컬 로그 수집으로 Panorama 가상 어플라이언스를 배포하려면 다음 단계를 수행하십시오. 이미 수행한 모든 단계(예: 초기 설정)를 건너뜁니다.

STEP 1 | 각 Panorama 가상 어플라이언스의 초기 설정을 수행합니다.

1. Panorama 가상 어플라이언스 설치. 가상 어플라이언스가 Panorama 모드에서 시작되도록 하려면 설치 중에 가상 로깅 디스크를 추가하지 마십시오.

   기본적으로 *Panorama*는 로그 저장을 위해 시스템 디스크의 *11GB* 파티션을 사용합니다. 더 많은 저장 공간을 원하시면 설치 후 최대 *8TB*의 전용 가상 로깅 디스크를 추가할 수 있습니다.
2. Panorama 가상 어플라이언스의 초기 구성 수행.
3. Panorama를 등록하고 라이선스를 설치합니다.
4. Panorama용 콘텐츠 및 소프트웨어 업데이트를 설치합니다.

STEP 2 | HA 구성에서 Panorama 가상 어플라이언스를 설정합니다.

1. Panorama에서 HA 설정.
2. Panorama HA 페일오버 테스트.

©2024 Palo Alto Networks, Inc.

STEP 3 | 로그 수집을 위해 Panorama를 준비하려면 다음 단계를 수행하십시오.

1. Panorama에 로그를 포워딩할 각 디바이스에 대해 방화벽을 관리 디바이스로 추가하십시오.
2. Panorama에 대한 로그 포워딩을 구성합니다.

STEP 4 | 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

Manage WildFire Appliances

Panorama M-시리즈 또는 가상 어플라이언스를 사용하여 최대 200개의 독립형 WildFire 어플라이언스 및 WildFire 어플라이언스 클러스터 노드를 중앙에서 관리할 수 있습니다. 로컬 CLI를 사용하여 WildFire 어플라이언스 및 어플라이언스 클러스터를 개별적으로 관리하는 것과 비교하여 Panorama를 사용하면 여러 어플라이언스 및 어플라이언스 클러스터에 대한 중앙 집중식 관리 및 모니터링을 제공합니다. 중앙 집중식 관리를 통해 관리되는 WildFire 어플라이언스의 전체 또는 하위 집합에 공통 구성, 구성 업데이트 및 소프트웨어 업그레이드를 푸시할 수 있으므로 WildFire 어플라이언스 및 어플라이언스 클러스터가 일관된 구성을 갖도록 쉽게 보장할 수 있습니다.

Panorama를 사용하여 WildFire 어플라이언스 클러스터를 관리하는 경우 Panorama는 관리 중인 WildFire 어플라이언스와 같거나 이후 버전을 실행해야 합니다.

- Panorama로 관리할 독립형 WildFire 어플라이언스 추가
- Panorama에서 기본 WildFire 어플라이언스 설정 구성
- WildFire 어플라이언스 및 클러스터에서 사용자 지정 인증서를 사용하여 인증 설정
- Panorama Management에서 WildFire 어플라이언스 제거
- WildFire 클러스터 관리

Panorama로 관리할 독립형 WildFire 어플라이언스 추가

Panorama® M-시리즈 또는 가상 어플라이언스로 최대 200개의 WildFire® 어플라이언스를 관리할 수 있습니다. WildFire 200 어플라이언스 한도는 독립 실행형 어플라이언스와 WildFire 어플라이언스 클러스터 노드를 합한 합계입니다(클러스터 구성 및 Panorama에서 노드 추가도 함께 수행하는 경우).

Panorama 서버가 PAN-OS® 8.1.0 이상의 버전을 실행 중이고 Panorama 관리 서버에 추가하는 WildFire 어플라이언스도 PAN-OS 8.1.0 이상의 버전을 실행 중인지 확인하십시오.

디바이스 등록 인증 키는 처음 연결할 때 Panorama 관리 서버와 WildFire 어플라이언스를 안전하게 인증하고 연결하는 데 사용됩니다. 디바이스 등록 인증 키를 구성하려면 키 수명과 인증 키를 사용하여 새 WildFire 어플라이언스를 온보딩할 수 있는 횟수를 지정하십시오. 또한 인증 키가 유효한 하나 이상의 WildFire 어플라이언스 일련번호를 지정할 수 있습니다.

인증 키는 키 수명이 만료된 후 90일이 지나면 만료됩니다. 90일이 지나면 유효성을 유지하기 위해 인증 키를 다시 인증하라는 메시지가 표시됩니다. 재인증을 하지 않으면 인증키가 무효가 됩니다. WildFire 어플라이언스가 Panorama 생성 인증 키를 사용할 때마다 시스템 로그가 생성됩니다. WildFire 어플라이언스는 이후의 모든 통신에 사용되는 디바이스 인증서를 전달할 때 인증 키를 사용하여 Panorama를 인증합니다.

PAN-OS 10.1 릴리즈를 실행하는 *WildFire* 어플라이언스의 경우 *PAN-OS 11.1*을 실행하는 *Panorama*는 *PAN-OS 10.1.3* 이상 릴리즈만 실행하는 *WildFire* 어플라이언스 온보딩을 지원합니다. *Panorama*가 *PAN-OS 11.1* 이상 릴리즈를 실행 중인 경우 *Panorama* 관리에 *PAN-OS 10.1.2* 또는 *PAN-OS 11.1* 이전 릴리즈를 실행하는 *WildFire* 어플라이언스는 추가할 수 없습니다.

*Panorama*는 다음 릴리스를 실행하는 온보딩 *WildFire* 어플라이언스를

- ***PAN-OS 10.2*** 이상 릴리스를 실행하는 ***Panorama*** - *PAN-OS 10.1.3* 이상 릴리스를 실행하는 와일드파이어 어플라이언스 및 *PAN-OS 10.0* 또는 이전 버전의 *PAN-OS* 릴리스를 실행하는 와일드파이어 어플라이언스

PAN-OS 10.2 이상 릴리스로 업그레이드해도 *Panorama*에서 이미 관리하는 *WildFire* 어플라이언스에는 영향이 없습니다.

STEP 1 | 로컬 CLI를 사용하여 Panorama 관리 서버에서 관리하려는 각 WildFire 어플라이언스가 PAN-OS 8.1.0 이상의 버전을 실행 중인지 확인합니다.

```
admin@qa16> show system info | match version sw-version: 11.0.0 wf-content-version: 702-283 logdb-version: 8.0.15
```

STEP 2 | WildFire 어플라이언스를 관리하는 데 사용할 각 Panorama 어플라이언스에서 Panorama 관리 서버가 PAN-OS 8.1.0 이상의 버전을 실행 중인지 확인하십시오.

대시보드 > 일반 정보 > 소프트웨어 버전은 실행 중인 소프트웨어 버전을 표시합니다.

STEP 3 | WildFire 어플라이언스가 WildFire 어플라이언스 클러스터에 속하는지 또는 로컬 WildFire 어플라이언스 CLI의 독립 실행형 어플라이언스인지 확실하지 않은 경우 ## ##를 확인하여 상태가

 ©2024 Palo Alto Networks, Inc.

`stand_alone`인지 확인하고 `Applicationstatus`가 `global-db-service` 및 `global-queue-service`는 `ReadyStandalone`을 나타내는지 확인합니다.

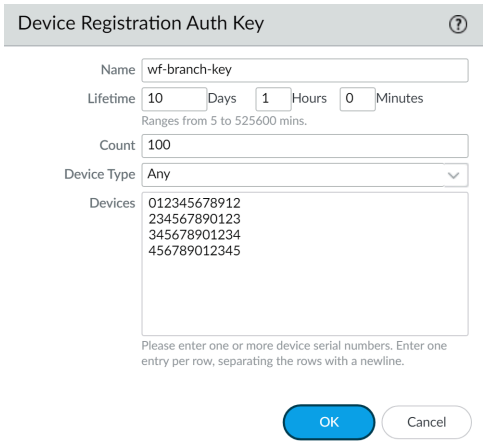
```
admin@WF-500> show cluster membership Service Summary: wfpc
 signature Cluster name: ##: 10.10.10.100 ### ##: WF-500 Node
 name: wfpc-012345678901-internal Serial number: 012345678901 #
# ##: stand_alone ## ##: ### HA ## ##: ### ##: Mon, 06 Mar 2017
 16:34:25 -0800 Services: wfcore signature wfpc infra Monitor
 status: Serf Health Status: passing Agent alive and reachable
 Application status: global-db-service: ReadyStandalone
           wildfire-apps-service: Ready  global-queue-service:
 ReadyStandalone                 wildfire-management-service:
 Done                  siggen-db: ReadyMaster Diag report:
 10.10.10.100: reported leader '10.10.10.100', age 0. 10.10.10.100:
 local node passed sanity check.
```

STEP 4 | Panorama로 관리하려는 WildFire 어플라이언스가 새 제품인 경우 WildFire 시작하기를 선택하여 WildFire 라이선스 활성화 확인, 로깅 활성화, WildFire 어플라이언스에 방화벽 연결, 기본 WildFire 기능 구성과 같은 기본 단계를 완료했는지 확인하십시오.

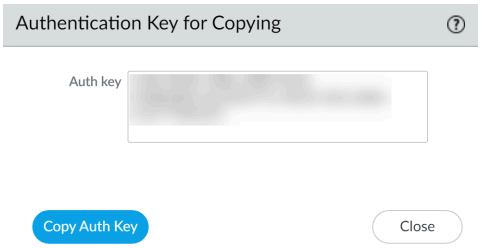
©2024 Palo Alto Networks, Inc.

STEP 5 | 기기 등록 인증 키를 생성합니다.

1. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
2. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 추가합니다.
   - 수명 - 새 **WildFire** 어플라이언스를 온보딩하는 데 사용되는 인증 키를 사용할 수 있는 기간에 대한 키 수명을 지정합니다.
   - 개수 - 인증 키를 사용하여 새 **WildFire** 어플라이언스를 온보딩할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 인증 키가 모든 디바이스를 인증하는 데 사용되도록 지정합니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 **WildFire** 어플라이언스를 지정하려면 하나 이상의 디바이스 일련번호를 입력합니다.
3. 확인을 클릭합니다.



4. 인증 키를 복사하고 닫습니다.



STEP 6 | 각 **WildFire** 어플라이언스의 로컬 **CLI**에서 **Panorama** 서버는 **Panorama** 서버의 **IP** 주소를 관리하고 구성하며 디바이스 등록 인증 키를 추가합니다.

독립형 **WildFire** 어플라이언스를 **Panorama** 어플라이언스에 등록하기 전에 먼저 **Panorama IP** 주소 또는 **FQDN**을 구성하고 각 **WildFire** 어플라이언스에 디바이스 등록 인증 키를 추가해야 합니다. 이를 통해 각 **WildFire** 어플라이언스는 **WildFire** 어플라이언스를 관리하는 **Panorama** 어플라이언스에 안

 ©2024 Palo Alto Networks, Inc.

전하게 연결할 수 있습니다. 디바이스 등록 인증 키는 Panorama 서버에 대한 초기 연결에만 사용됩니다.

1. 기본 Panorama 서버에 대한 관리 인터페이스의 IP 주소 또는 FQDN을 구성합니다.

```
admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
```

2. 고가용성을 위해 백업 Panorama 어플라이언스를 사용하는 경우(권장), 백업 Panorama 서버에 대한 관리 인터페이스의 IP 주소 또는 FQDN을 구성합니다.

```
admin@WF-500# set deviceconfig system panorama-server-2 <ip-address | FQDN>
```

3. 디바이스 등록 인증 키를 추가합니다.

```
admin> ## # ## <auth-key> ##
```



STEP 7 | 기본 Panorama 어플라이언스에 WildFire 어플라이언스를 등록합니다.

1. Panorama 웹 인터페이스에서 **Panorama** > **Managed WildFire Appliances** 및 **Add Appliance**
2. 별도의 줄에 각 WildFire 어플라이언스의 일련번호를 입력합니다. 일련번호 목록이 없는 경우 각 WildFire 어플라이언스에서 다음을 실행합니다.

```
admin@WF-500> show system info | match serial serial:
 012345678901
```

   여러 로컬 CLI 명령은 #### ### ##를 포함하여 WildFire 어플라이언스 일련번호를 표시합니다.
3. 확인을 클릭합니다.

   사용 가능한 경우 IP 주소 및 소프트웨어 버전과 같이 WildFire 어플라이언스에서 이미 커밋된 구성에 대한 정보가 표시됩니다.

STEP 8 | (선택 사항) WildFire 어플라이언스 구성을 Panorama 어플라이언스로 가져옵니다.

1. 관리되는 WildFire 어플라이언스 목록에서 가져올 구성이 있는 어플라이언스를 선택하십시오.
2. 구성을 가져옵니다.
3. 예를 선택합니다.

   구성을 가져오면 표시된 정보가 업데이트되고 가져온 구성이 Panorama 어플라이언스 후보 구성의 일부가 됩니다.
4. 불러온 WildFire 어플라이언스 구성을 Panorama 실행 구성의 일부로 만들려면 **Panorama**에 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | WildFire 어플라이언스 인터페이스의 구성을 구성하거나 확인합니다.

각 WildFire 어플라이언스에는 4개의 인터페이스가 있습니다. 관리(Ethernet0), 분석 네트워크 환경(Ethernet1), **Ethernet2** 및 **Ethernet3**.

1. **Panorama** > **Managed WildFire** 어플라이언스를 선택하고 WildFire 어플라이언스를 선택합니다.
2. 인터페이스를 선택합니다.
3. 구성하거나 편집할 인터페이스를 선택합니다. 인터페이스를 활성화하고, 속도 및 이중 방식을 설정하고, 각 인터페이스에 대한 IP 주소 및 넷마스크, 기본 게이트웨이, MTU, DNS 서버, 링크 상태 및 관리 서비스를 구성할 수 있습니다. 인터페이스가 지정된 주소의 트래픽만 수락하도록 허용된 IP 주소를 추가할 수도 있습니다.

   분석 네트워크 환경, 이더넷**2** 및 이더넷**3** 인터페이스는 관리 서비스 옵션으로 **Ping**만 지원합니다.

   관리 인터페이스는 관리 서비스 옵션으로 **Ping**, **SSH** 및 **SNMP**를 지원합니다. 또한 관리 인터페이스는 인터넷에 직접 연결할 수 없는 경우 프록시 서버 구성을 지원합니다.
4. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 10 | Panorama 어플라이언스에서 구성을 커밋하고 어플라이언스 또는 여러 어플라이언스에 푸시합니다.

1. 커밋하고 푸시합니다.
2. Panorama 어플라이언스에 푸시하지 않으려는 구성이 있는 경우 선택 편집을 클릭하여 구성을 푸시할 어플라이언스를 선택합니다. 푸시된 구성은 WildFire 어플라이언스에서 실행 중인 구성을 덮어씁니다.

STEP 11 | 구성을 확인합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택합니다.
2. 다음 필드를 확인하십시오.
   - 연결됨 - 상태가 연결됨입니다.
   - 역할 - 각 WildFire 어플라이언스의 역할은 독립 실행형입니다.
   - 구성 상태 - 상태가 `InSync`입니다.
   - 마지막 커밋 상태 - ## ##.

 ©2024 Palo Alto Networks, Inc.

Panorama에서 기본 WildFire 기기 설정 구성

콘텐츠 업데이트 및 WildFire 클라우드 서버, WildFire 클라우드 서비스, 로깅, 인증 등의 기본 설정을 구성하는 것은 Panorama에서 일반 클러스터 설정을 구성하는 방법과 유사합니다. 클러스터를 선택하고 클러스터에서 설정을 구성하는 대신 WildFire 어플라이언스를 선택하고 해당 어플라이언스에 대한 개별 설정을 구성하십시오. Panorama에 추가하는 각 WildFire 어플라이언스를 선택하고 구성합니다.

WildFire 어플라이언스 구성에서는 WildFire 어플라이언스를 네트워크에 통합하고 CLI를 사용하여 기본 설정을 수행하는 방법을 설명하지만 개념은 Panorama를 사용하여 기본 설정을 수행하는 것과 동일합니다.

많은 설정이 기본값, *WildFire* 어플라이언스의 이전 기존 설정 정보 또는 *WildFire* 어플라이언스를 *Panorama*에 추가할 때 구성한 설정으로 미리 채워져 있습니다.

- WildFire 어플라이언스에 대한 인증 구성

WildFire 어플라이언스에 대한 인증 구성

세분화된 인증 매개변수를 사용하여 로컬 관리 사용자를 구성하고 권한 부여 및 인증을 위해 RADIUS, TACAS+ 또는 LDAP를 활용하여 WildFire 어플라이언스에 대한 향상된 인증을 생성 및 구성합니다.

Panorama에서 관리자를 구성하고 푸시하면 WildFire 어플라이언스의 기존 관리자를 Panorama에서 구성한 관리자로 덮어씁니다.

- WildFire 어플라이언스에 대한 관리 계정 구성
- WildFire 어플라이언스에 대한 RADIUS 인증 구성
- WildFire 어플라이언스에 대한 TACACS+ 인증 구성
- WildFire 어플라이언스에 대한 LDAP 인증 구성

WildFire 어플라이언스에 대한 관리 계정 구성

Panorama™ 관리 서버에서 관리할 WildFire 어플라이언스에 대한 세분화된 인증 매개변수를 사용하여 한 명 이상의 관리자를 만드십시오. 또한 WildFire 어플라이언스의 CLI에서 직접 구성할 수 있는 Panorama에서 로컬 관리자를 구성할 수 있습니다. 그러나 WildFire 어플라이언스에 새 구성 변경 사항을 푸시하면 WildFire 어플라이언스에 대해 구성된 관리자가 로컬 관리자를 덮어씁니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama로 관리할 독립형 WildFire 어플라이언스 추가.

STEP 3 | (선택 사항) WildFire 어플라이언스 CLI에 액세스하는 관리자의 로그인 자격 증명을 확인하는 인증 서비스를 정의하도록 인증 프로파일을 구성합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | 필요에 따라 하나 이상의 관리자 계정을 구성합니다.

Panorama에서 생성된 관리자 계정은 나중에 WildFire 어플라이언스로 가져와 Panorama에서 관리됩니다.

WildFire 어플라이언스에 대한 인증을 성공적으로 구성하려면 운용 관리자 역할 권한이 있는 관리 계정을 구성해야 합니다.

STEP 5 | WildFire 어플라이언스에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 이전에 추가한 WildFire 어플라이언스를 선택합니다.
2. (선택 사항) 이전 단계에서 구성한 인증 프로파일을 선택합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

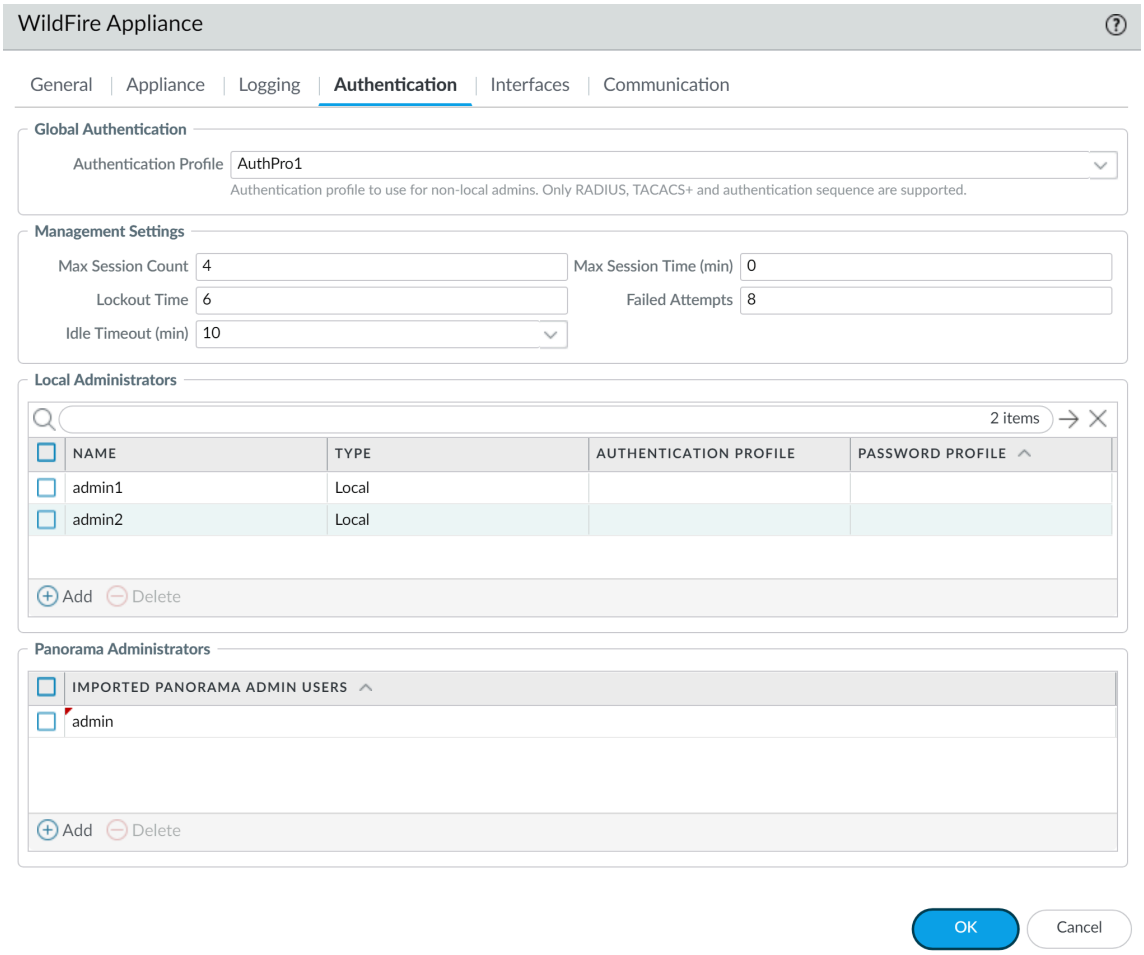
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 WildFire 어플라이언스에만 해당되며 이 표에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되어 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 어플라이언스 인증 구성을 저장합니다.



STEP 6 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 7 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 어플라이언스에 대한 RADIUS 인증 구성

RADIUS 서버를 사용하여 WildFire 어플라이언스 CLI에 대한 관리 액세스를 인증합니다. RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama™ 관리 서버에서 설정을 재구성하는 것보다 훨씬 쉽습니다.

©2024 Palo Alto Networks, Inc.

Palo Alto Networks RADIUS 사전을 *RADIUS* 서버로 가져와 *Panorama*와 *RADIUS* 서버 간의 통신에 필요한 인증 속성을 정의할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama로 관리할 독립형 WildFire 어플라이언스 추가.

STEP 3 | RADIUS 인증을 구성합니다.

Wildfire 어플라이언스에 대한 인증을 성공적으로 구성하려면 *RADIUS* 인증을 위해 구성된 관리자 계정에 운용 관리자 역할 권한이 있어야 합니다.

1. RADIUS 서버 프로파일을 추가합니다.

   프로파일은 WildFire 어플라이언스가 RADIUS 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server Profiles** > **RADIUS**를 선택하고 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 1–20 범위).
   4. WildFire 어플라이언스가 RADIUS 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

      RADIUS 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.

   5. 각 RADIUS 서버를 추가하고
      1. 서버를 식별할 이름을 입력합니다.
      2. **RADIUS** 서버 IP 주소 또는 FQDN.
      3. 암호/암호 확인(사용자 이름과 암호를 암호화하는 키)
      4. 인증 요청을 위한 서버 포트(기본값은 1812).
   6. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. RADIUS 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
   2. 인증 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **RADIUS**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. **RADIUS**에서 사용자 그룹 검색을 선택하여 RADIUS 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 어플라이언스에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 이전에 추가한 WildFire 어플라이언스를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

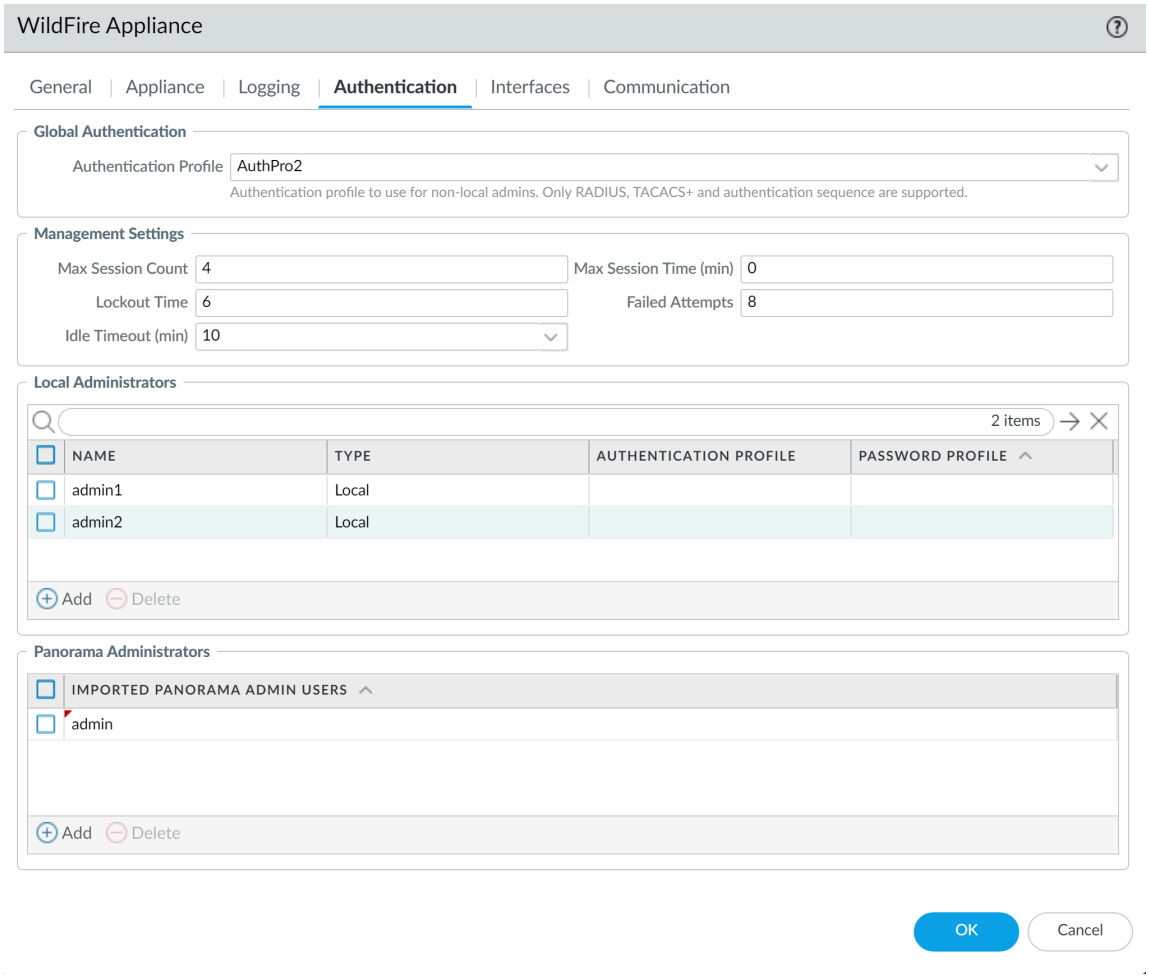
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 WildFire 어플라이언스에만 해당되며 이 표에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되어 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 어플라이언스 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 어플라이언스에 대한 TACACS+ 인증 구성

TACACS+ 서버를 사용하여 WildFire 어플라이언스 CLI에 대한 관리 액세스를 인증할 수 있습니다. TACACS+ 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama로 관리할 독립형 WildFire 어플라이언스 추가.

STEP 3 | TACACS+ 인증을 구성합니다.

TACACS+ 인증을 위해 구성된 관리자 계정은 *Wildfire* 어플라이언스에 대한 인증을 성공적으로 구성하려면 운용 관리자 관리자 역할 권한이 있어야 합니다.

1. TACACS+ 서버 프로파일을 추가합니다.

   프로파일은 WildFire 어플라이언스가 TACACS+ 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server Profiles** > **TACACS+**를 선택한 다음 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).
   4. Panorama가 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.
   5. TACACS+ 서버가 해당 프로토콜을 지원하는 경우 **CHAP**를 선택하십시오. **PAP**보다 더 안전합니다.
   6. 각 TACACS+ 서버를 추가하고 서버를 식별할

      1. 이름을 입력합니다.
      2. **TACACS+** 서버 IP 주소 또는 FQDN.
      3. 암호/암호 확인(사용자 이름과 암호를 암호화하는 키).
      4. 인증 요청을 위한 서버 포트(기본값은 49).
   7. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택한 다음 프로파일을 추가합니다.
   2. 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **TACACS+**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집하려면 TACACS+에서 사용자 그룹 검색을 선택합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 어플라이언스에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 이전에 추가한 WildFire 어플라이언스를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

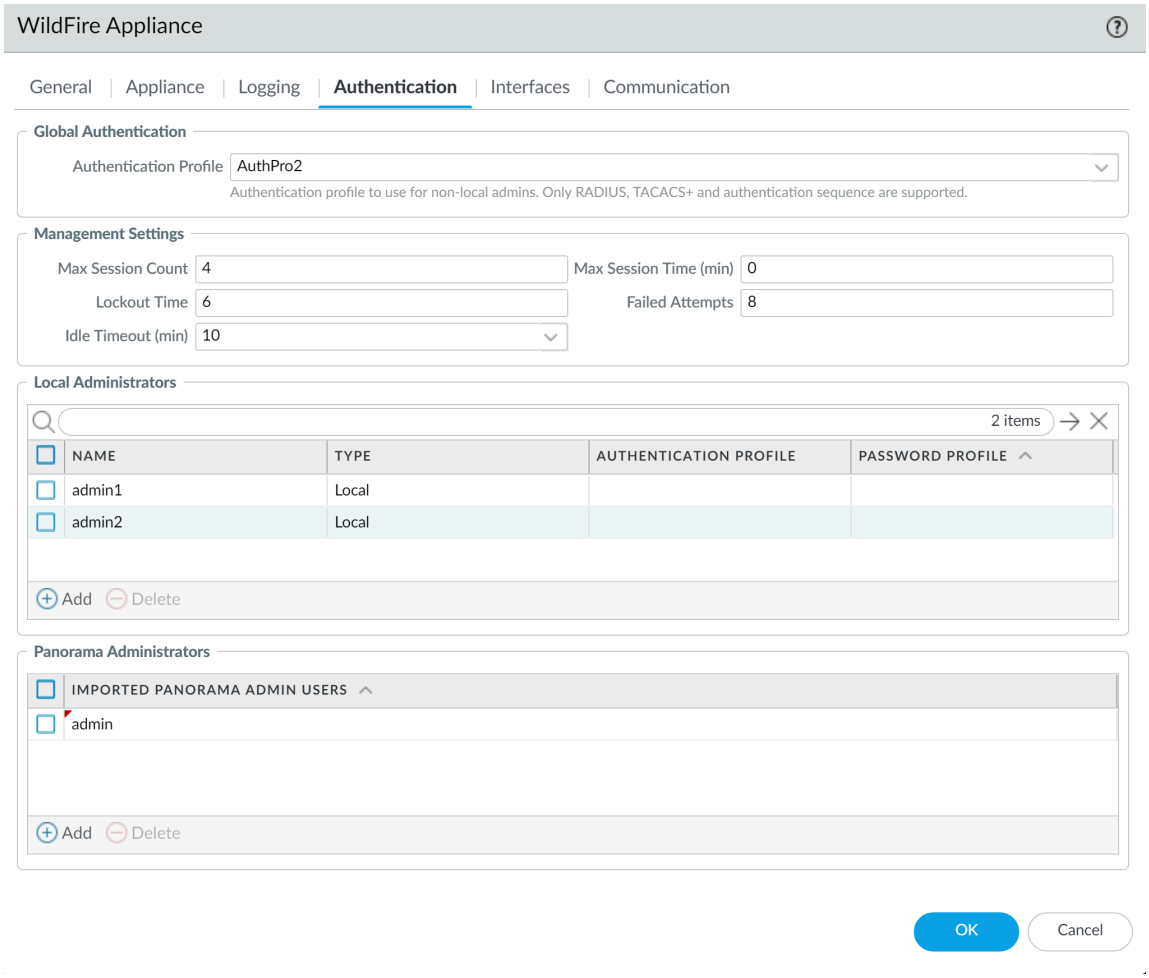
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 생성된 WildFire 어플라이언스에만 해당되며 이 표에서 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되어 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 어플라이언스 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 어플라이언스에 대한 LDAP 인증 구성

LDAP를 사용하여 WildFire 어플라이언스 CLI에 액세스하는 최종 사용자를 인증할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama로 관리할 독립형 WildFire 어플라이언스 추가.

©2024 Palo Alto Networks, Inc.

STEP 3 | LDAP 서버 프로파일을 추가합니다.

프로파일은 WildFire 어플라이언스가 LDAP 서버에 연결하는 방법을 정의합니다.

WildFire 어플라이언스에 대한 인증을 성공적으로 구성하려면 *LDAP* 인증을 위해 구성된 관리자 계정에 운용 관리자 역할 권한이 있어야 합니다.

1. **Panorama** > 서버 프로파일 > **LDAP** 및 서버 프로파일 추가를 선택합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. LDAP 서버를 추가합니다(최대 4개). 각 서버에 대해 이름(서버 식별), **LDAP** 서버 IP 주소 또는 FQDN 및 서버 포트(기본값 389)를 입력합니다.

   FQDN 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소에 대한 변경 사항을 적용해야 합니다.
4. 서버 유형을 선택합니다.
5. 기본 **DN**을 선택합니다.

   디렉터리의 기본 DN을 식별하려면 **Active Directory** 도메인 및 트러스트 Microsoft 관리 콘솔 스냅인을 열고 최상위 도메인의 이름을 사용합니다.
6. 바인딩 **DN** 및 암호를 입력하여 인증 서비스에서 방화벽을 인증할 수 있도록 합니다.

   Bind DN 계정에는 *LDAP* 디렉토리를 읽을 수 있는 권한이 있어야 합니다.
7. 바인딩 타임아웃 및 검색 타임아웃(초)을 입력합니다. 기본값은 모두 30입니다.
8. 재시도 간격(초)을 입력합니다(기본값은 60).
9. (선택 사항) 엔드포인트가 디렉터리 서버와의 보다 안전한 연결을 위해 SSL 또는 TLS를 사용하도록 하려면 **SSL/TLS** 보안 연결 필요(기본적으로 활성화됨) 옵션을 활성화합니다. 엔드포인트가 사용하는 프로토콜은 서버 포트에 따라 다릅니다.
   - 389(기본값) - TLS(특히 WildFire 어플라이언스는 StartTLS 작업을 사용하여 초기 일반 텍스트 연결을 TLS로 업그레이드합니다.)
   - 636—SSL
   - 기타 포트 - WildFire 어플라이언스는 먼저 TLS 사용을 시도합니다. 디렉토리 서버가 TLS를 지원하지 않는 경우 WildFire 어플라이언스는 SSL로 대체합니다.
10. (선택 사항) 보안을 강화하려면 SSL/TLS 연결에 대해 디렉터리 서버가 제공하는 인증서를 엔드포인트에서 확인할 수 있도록 **SSL** 세션에 대한 서버 인증서 확인 옵션을 활성화합니다. 확인을 활성화하려면 **SSL/TLS** 보안 연결 필요 옵션도 활성화해야 합니다. 확인이 성공하려면 인증서가 다음 조건 중 하나를 충족해야 합니다.
    - Panorama 인증서 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서 > 디바이스 인증서. 필요한 경우 인증서를 Panorama로 가져옵니다.
    - 인증서 서명자는 신뢰할 수 있는 인증 기관 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서.
11. 확인을 클릭하여 서버 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 어플라이언스에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 이전에 추가한 WildFire 어플라이언스를 선택합니다.
2. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
3. WildFire 어플라이언스 관리자를 추가합니다.

   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

- 로컬 관리자를 구성합니다.

  WildFire 어플라이언스에 고유한 새 관리자를 구성합니다. 이러한 관리자는 생성된 WildFire 어플라이언스에만 해당되며 이 표에서 관리자를 관리합니다.

  1. 한 명 이상의 새 로컬 관리자를 추가하십시오.
  2. 로컬 관리자의 이름을 입력합니다.
  3. 이전에 생성한 인증 프로파일을 할당합니다.

     LDAP 인증 프로파일은 개별 로컬 관리자에 대해서만 지원됩니다.

  4. 인증을 위해 공개 키 파일을 가져오려면 공개 키 인증**(SSH)** 사용을 활성화(선택)합니다.
  5. 암호 프로파일을 선택하여 만료 매개변수를 설정합니다.

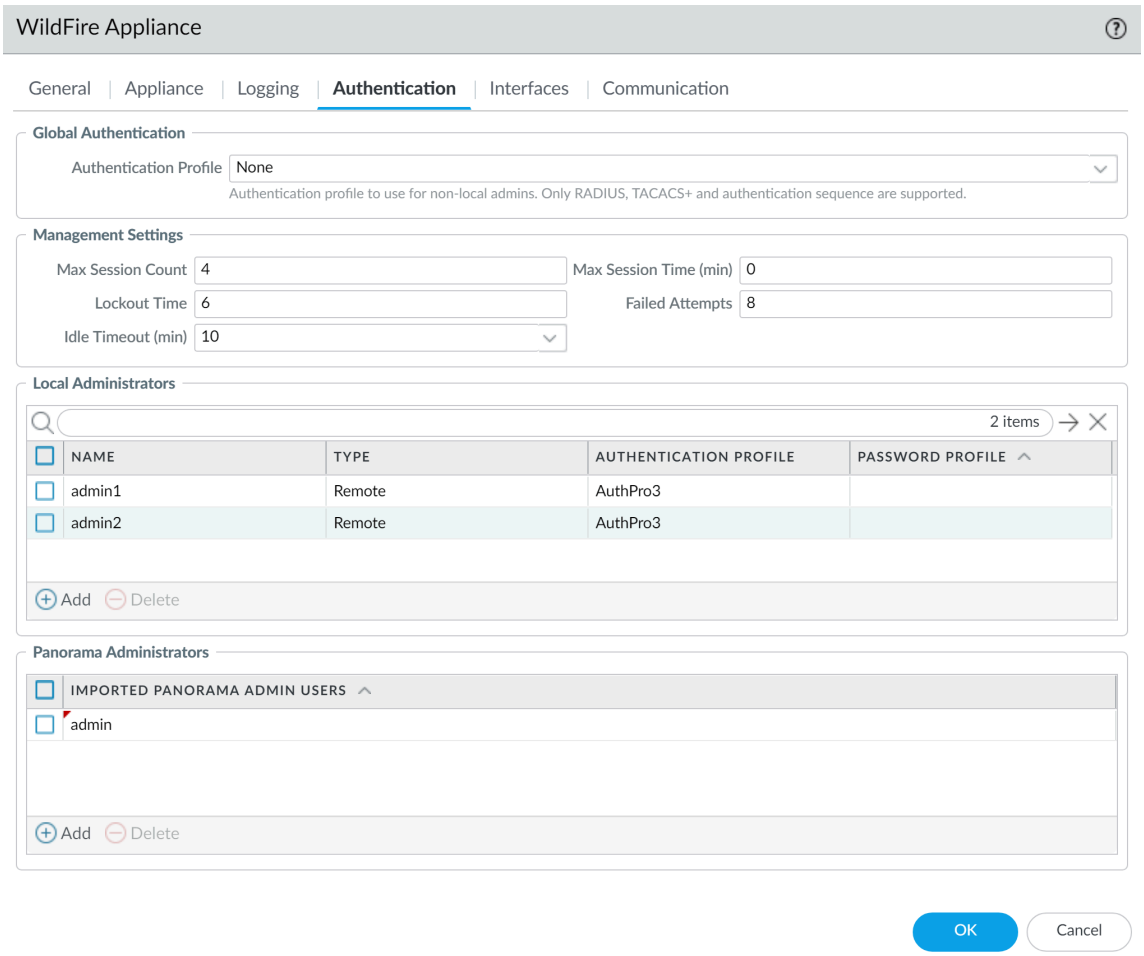
- 기존 Panorama 관리자 가져오기

  Panorama에 구성된 기존 관리자를 가져옵니다. 이러한 관리자는 Panorama에서 구성 및 관리되며 WildFire 어플라이언스로 가져옵니다.

  1. 기존 Panorama 관리자 추가

4. 확인을 클릭하여 WildFire 어플라이언스 인증 구성을 저장합니다.

 ©2024 Palo Alto Networks, Inc.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 **WildFire** 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

©2024 Palo Alto Networks, Inc.

WildFire 어플라이언스 및 클러스터에서 사용자 지정 인증서를 사용하여 인증 설정

기본적으로 WildFire® 어플라이언스는 다른 Palo Alto Networks® 방화벽 및 어플라이언스와의 상호 인증을 위해 사전 정의된 인증서를 사용하여 관리 액세스 및 디바이스 간 통신에 사용되는 SSL 연결을 설정합니다. 그러나 대신 사용자 지정 인증서를 사용하여 인증을 구성할 수 있습니다. 사용자 지정 인증서를 사용하면 Panorama™에서 관리하는 WildFire 어플라이언스 또는 WildFire 클러스터와 방화벽 간의 상호 인증을 보장하기 위해 고유한 신뢰 체인을 설정할 수 있습니다. 이러한 인증서는 Panorama 또는 방화벽에서 로컬로 생성하거나 신뢰할 수 있는 타사 인증 기관(CA)에서 얻거나 엔터프라이즈 PKI(개인 키 인프라)에서 인증서를 얻을 수 있습니다.

사용자 지정 인증서 사용에 대한 자세한 내용은 SSL/TLS 연결이 상호 인증되는 방법을 참조하십시오.

- Panorama Managed WildFire 어플라이언스에 대한 사용자 지정 인증서 구성
- WildFire 클러스터에 대한 단일 사용자 지정 인증서로 인증 구성
- Panorama를 통해 구성된 WildFire 어플라이언스에 사용자 지정 인증서 적용

Panorama Managed WildFire 어플라이언스에 대한 사용자 지정 인증서 구성

Panorama™를 사용하여 WildFire® 어플라이언스 또는 WildFire 클러스터를 관리하는 경우 WildFire 어플라이언스 CLI를 사용하는 대신 Panorama 웹 인터페이스를 통해 사용자 지정 인증서 인증을 구성할 수 있습니다. 방화벽 또는 Panorama는 이 연결을 사용하여 분석을 위해 샘플을 WildFire로 포워딩합니다.

이 절차에서는 단일 WildFire 어플라이언스에 고유 인증서를 설치하는 방법을 설명합니다. WildFire 어플라이언스가 클러스터의 일부인 경우 해당 디바이스와 각 클러스터 구성원에는 고유한 클라이언트 인증서가 있습니다. 클러스터의 모든 WildFire 어플라이언스에 단일 인증서를 배포하려면 WildFire 클러스터에 대한 단일 사용자 지정 인증서로 인증 구성을 참조하십시오.

STEP 1 | WildFire 어플라이언스 및 방화벽에 대한 키 쌍 및 인증 기관(CA) 인증서를 가져옵니다.

STEP 2 | CA 인증서를 가져와서 WildFire 어플라이언스에 대한 방화벽 및 키 쌍의 ID를 확인합니다.

1. **Panorama** > 인증서 관리 > 인증서 > 가져오기를 선택합니다.
2. Panorama에서 CA 인증서와 키 쌍을 가져옵니다.

STEP 3 | 루트 CA 및 중간 CA를 포함하는 인증서 프로파일을 구성합니다. 이 인증서 프로파일은 WildFire 어플라이언스와 방화벽이 상호 인증하는 방법을 정의합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

   인증서 프로파일의 일부로 중간 CA를 구성하는 경우 루트 CA도 포함해야 합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 어플라이언스에 대한 SSL/TLS 프로파일을 구성합니다.

PAN-OS 8.0 이상의 버전는 *TLS 1.2* 이상만 지원하므로 최대 버전을 ***TLS 1.2*** 또는 최대로 설정해야 합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. WildFire 어플라이언스 및 해당 방화벽이 SSL/TLS 서비스에 사용하는 인증서와 프로토콜을 정의하도록 SSL/TLS 서비스 프로파일을 구성합니다.

STEP 5 | WildFire에서 보안 서버 통신을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터 또는 **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 클러스터 또는 어플라이언스를 선택합니다.
2. 통신을 선택합니다.
3. 보안 서버 통신 사용자 지정 기능을 활성화합니다.
4. **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 WildFire 어플라이언스와 방화벽 또는 Panorama 간의 모든 SSL 연결에 적용됩니다.
5. WildFire 어플라이언스와 방화벽 또는 Panorama 간의 통신을 위해 구성한 인증서 프로파일을 선택합니다.
6. 사용자 지정 인증서만 비활성화(선택 취소)되었는지 확인합니다. 이를 통해 WildFire 어플라이언스는 사용자 지정 인증서로 마이그레이션하는 동안 사전 정의된 인증서를 사용하여 방화벽과 계속 통신할 수 있습니다.
7. (선택 사항) 권한 부여 목록을 구성합니다.
   1. 권한 부여 목록을 추가합니다.
   2. 인증서 프로파일에 구성된 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 식별자가 제목인 경우 일반 이름을 입력하거나 식별자가 제목 대체 이름인 경우 IP 주소, 호스트 이름 또는 이메일을 입력합니다.
   4. 확인을 클릭합니다.
   5. 목록을 적용하려면 승인 목록 확인을 활성화하십시오.
8. 확인을 클릭합니다.
9. 변경 사항을 커밋합니다.

STEP 6 | CA 인증서를 가져와서 WildFire 어플라이언스에 대한 인증서를 확인합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. CA 인증서를 가져옵니다.

STEP 7 | 방화벽에 대한 로컬 또는 SCEP 인증서를 구성합니다.

- 로컬 인증서를 사용하는 경우 방화벽에 대한 키 쌍을 가져옵니다.
- 방화벽 인증서에 SCEP를 사용하는 경우 SCEP 프로파일을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 방화벽 또는 Panorama에 대한 인증서 프로파일을 구성합니다. 각 클라이언트 방화벽 또는 Panorama 어플라이언스에서 이 프로파일을 개별적으로 구성하거나 템플릿을 사용하여 Panorama에서 관리 방화벽으로 구성을 푸시할 수 있습니다.

1. 방화벽의 경우 디바이스 > 인증서 관리 > 인증서 프로파일을 선택한 다음 Panorama의 경우 **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

STEP 9 | 각 방화벽 또는 Panorama 어플라이언스에 사용자 지정 인증서를 배포합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 방화벽의 경우 디바이스 > 설정 > 관리를 선택하고 Panorama의 경우 **Panorama** > 설정 > 관리를 선택하고 통신 보안 설정을 편집합니다.
3. 인증서 유형, 인증서 및 인증서 프로파일을 선택합니다.
4. 통신 사용자 정의 설정에서 **WildFire** 통신을 선택합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

STEP 10 | 모든 관리 디바이스에 사용자 지정 인증서를 배포한 후 사용자 지정 인증서 인증을 시행합니다.

1. Panorama에 로그인합니다.
2. **Panorama** > 관리형 **WildFire** 클러스터 또는 **Panorama** > 관리형 **WildFire** 어플라이언스를 선택하고 클러스터 또는 어플라이언스를 선택합니다.
3. 통신을 선택합니다.
4. 사용자 지정 인증서만을 선택합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

이 변경 사항을 커밋한 후 WildFire는 즉시 사용자 지정 인증서 시행을 시작합니다.

WildFire 클러스터에 대한 단일 사용자 지정 인증서로 인증 구성

클러스터의 각 WildFire® 어플라이언스에 고유한 인증서를 할당하는 대신 전체 WildFire 클러스터에 단일 공유 클라이언트 인증서를 할당할 수 있습니다. 각 클러스터 구성원에 대해 별도의 인증서를 구성합니다. 개별 WildFire 어플라이언스는 클라이언트 인증서를 공유하므로 각 WildFire 어플라이언스에 대해 고유한 호스트 이름(DNS 이름)을 구성해야 합니다. 그런 다음 모든 호스트 이름을 인증서 속성으로 공유 인증서에 추가하거나 클러스터의 모든 WildFire 어플라이언스에 있는 모든 사용자 지정 호스트 이름과 일치하는 단일 와일드카드 문자열을 사용할 수 있습니다.

Panorama™와 통신할 때 사용할 WildFire 클러스터용 단일 사용자 지정 인증서를 구성하려면 다음 절차를 완료하십시오.

STEP 1 | Panorama용 서버 키 쌍 및 CA 인증서를 얻습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 루트 CA(인증 기관) 및 중간 CA를 포함하는 인증서 프로필을 구성합니다. 이 인증서 프로파일은 WildFire 클러스터(클라이언트)와 Panorama 어플라이언스(서버) 간의 인증을 정의합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

   인증서 프로파일의 일부로 중간 CA를 구성하는 경우 루트 CA도 포함해야 합니다.

STEP 3 | SSL/TLS 서비스 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. WildFire 클러스터 및 Panorama 어플라이언스가 SSL/TLS 서비스에 사용하는 인증서와 프로토콜을 정의하도록 SSL/TLS 서비스 프로파일을 구성합니다.

STEP 4 | 클러스터의 각 노드를 Panorama에 연결합니다.

STEP 5 | 클러스터의 각 노드에서 고유한 호스트 이름(DNS 이름)을 구성하거나 클러스터의 WildFire 어플라이언스에 설정된 모든 사용자 정의 DNS 이름과 일치하는 단일 와일드카드가 있는 문자열을 사용하십시오.

단일 와일드카드 문자열을 사용하는 경우 와일드카드 문자열 값의 요구 사항 및 제한 사항은 RFC-6125, 섹션 6.4.3을 참조하십시오. 사용자 지정 DNS 이름을 구성할 때 이러한 요구 사항과 제한 사항을 이해해야 합니다.

1. 노드에서 WildFire CLI에 로그인합니다.
2. 다음 명령을 사용하여 노드에 고유한 사용자 지정 DNS 이름을 할당합니다.

```
admin@WF-500> configure
```

```
admin@WF-500# set deviceconfig setting wildfire custom-dns-name <dns-name>
```

3. 변경사항을 커밋합니다.
4. 클러스터의 각 노드에 대해 이 프로세스를 반복합니다.

STEP 6 | Panorama에서 클러스터의 모든 노드에 대한 클라이언트 인증서를 생성합니다. 인증서 속성 아래에서 클러스터 노드에 할당한 각 사용자 지정 DNS 이름에 대한 호스트 이름 항목을 추가하거나 *.example.com과 같이 모든 노드 호스트 이름과 일치하는 하나의 와일드카드 문자열이 있는 하나의 호스트 이름 항목을 추가합니다. 각 사용자 지정 DNS 이름이 공통 문자열을 공유하는 경우에만 이 작업을 수행할 수 있습니다.

STEP 7 | Panorama에서 클러스터 클라이언트 인증서에 대한 인증서 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **Panorama**에 대한 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | 각 노드에 사용자 지정 인증서를 배포합니다. 이 인증서 프로필에는 Panorama 서버 인증서에 서명한 CA 인증서가 포함되어야 합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택한 다음 클러스터 이름을 클릭합니다.
2. 통신을 선택합니다.
3. 보안 클라이언트 통신에서 인증서 유형, 인증서 및 인증서 프로파일을 선택합니다.
4. 확인을 클릭합니다.
5. 변경 사항을 커밋합니다.

STEP 9 | Panorama에서 보안 서버 통신을 구성합니다.

1. **Panorama** > 설정 > 관리 및 편집을 선택하여 보안 서버 통신 사용자 지정을 선택합니다.
2. 보안 서버 통신 사용자 지정을 활성화합니다.
3. **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL / TLS 서비스 프로파일은 WildFire와 Panorama 간의 모든 SSL 연결에 적용됩니다.
4. Panorama에 대한 인증서 프로파일을 선택합니다.
5. 사용자 지정 인증서만 활성화합니다.
6. 확인을 클릭합니다.
7. 변경 사항을 커밋합니다.

Panorama를 통해 구성된 WildFire 어플라이언스에 사용자 지정 인증서 적용

기본적으로 Panorama™는 구성을 푸시하기 위해 WildFire® 어플라이언스와 통신할 때 사전 정의된 인증서를 사용합니다. 또는 Panorama가 관리되는 WildFire 어플라이언스 또는 클러스터에 구성을 푸시하는 데 사용하는 연결에 대한 상호 인증을 설정하도록 사용자 지정 인증서를 구성할 수 있습니다. Panorama에서 서버 인증서를 구성하고 WildFire 어플라이언스에서 클라이언트 인증서를 구성하려면 다음 절차를 완료하십시오.

STEP 1 | Panorama 및 WildFire 어플라이언스에 대한 키 쌍 및 인증 기관(CA) 인증서를 가져옵니다.

STEP 2 | CA 인증서를 가져와서 WildFire 어플라이언스의 식별과 Panorama용 키 쌍을 확인합니다.

1. **Panorama** > 인증서 관리 > 인증서 > 가져오기를 선택합니다.
2. Panorama에서 CA 인증서와 키 쌍을 가져옵니다.

STEP 3 | 루트 CA 및 중간 CA를 포함하는 인증서 프로파일을 구성합니다. 이 인증서 프로파일은 WildFire 어플라이언스(클라이언트)와 Panorama 가상 또는 M-시리즈 어플라이언스(서버) 간의 인증을 정의합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

   인증서 프로파일의 일부로 중간 CA를 구성하는 경우 루트 CA도 포함해야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | SSL/TLS 서비스 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. WildFire 및 Panorama 어플라이언스가 SSL/TLS 서비스에 사용하는 인증서와 프로토콜을 정의하도록 SSL/TLS 서비스 프로파일을 구성합니다.

STEP 5 | Panorama 어플라이언스에서 보안 서버 통신을 구성합니다.

1. **Panorama** > 설정 > 관리 및 편집을 선택하여 보안 서버 통신 사용자 지정을 선택합니다.
2. 보안 서버 통신 사용자 지정 기능을 활성화합니다.
3. **SSL/TLS** 서비스 프로파일을 선택합니다.
4. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
5. 사용자 지정 인증서만 비활성화(선택 취소)되었는지 확인합니다. 이를 통해 Panorama는 사용자 정의 인증서로 마이그레이션하는 동안 사전 정의된 인증서로 WildFire와 계속 통신할 수 있습니다.
6. (선택 사항) 권한 부여 목록을 구성합니다.
   1. 권한 부여 목록을 추가합니다.
   2. 인증서 프로파일에 구성된 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 식별자가 ##인 경우 일반 이름을 입력하고 식별자가 ## ## ##인 경우 **IP** 주소, 호스트 이름 또는 이메일을 입력합니다.
   4. 확인을 클릭합니다.
   5. 권한 부여 목록 확인 옵션을 활성화하여 권한 부여 목록을 적용하도록 Panorama를 구성하십시오.
7. 확인을 클릭합니다.
8. 변경 사항을 커밋합니다.

STEP 6 | CA 인증서를 가져와 Panorama에서 인증서의 유효성을 검사합니다.

1. Panorama 사용자 인터페이스에 로그인합니다.
2. CA 인증서를 가져옵니다.

STEP 7 | WildFire 어플라이언스에 대한 로컬 또는 SCEP 인증서를 구성합니다.

1. 로컬 인증서를 사용하는 경우 WF-500 어플라이언스에 대한 키 쌍을 가져옵니다.
2. WildFire 어플라이언스 인증서에 SCEP를 사용하는 경우 SCEP 프로파일을 구성합니다.

STEP 8 | WildFire 어플라이언스에 대한 인증서 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

©2024 Palo Alto Networks, Inc.

STEP 9 | 각 관리형 WildFire 어플라이언스에 사용자 지정 인증서를 배포합니다.

1. Panorama에 로그인합니다.
2. **Panorama** > 관리형 **WildFire Appliances**를 선택하고 클러스터 또는 어플라이언스 이름을 클릭합니다.
3. 통신을 선택합니다.
4. 보안 클라이언트 통신 아래의 해당 드롭다운에서 인증서 유형, 인증서 및 인증서 프로파일을 선택합니다.
5. 확인을 클릭합니다.
6. 변경 사항을 커밋합니다.

STEP 10 | 모든 관리형 WildFire 어플라이언스에 사용자 지정 인증서를 배포한 후 사용자 지정 인증서 인증을 시행합니다.

1. **Panorama** > 설정 > 관리를 선택하고 통신 보안 설정을 편집합니다.
2. 사용자 지정 인증서만 허용합니다.
3. 확인을 클릭합니다.
4. 변경 사항을 커밋합니다.

이 변경 사항을 커밋한 후 연결 해제 대기 시간이 카운트다운되기 시작합니다. 대기 시간이 끝나면 Panorama와 관리되는 WildFire 어플라이언스는 구성된 인증서 없이 연결할 수 없습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama Management에서 WildFire 어플라이언스 제거

Panorama 관리에서 WildFire 독립 실행형 어플라이언스를 제거할 수 있습니다. Panorama 관리에서 독립형 WildFire 어플라이언스를 제거하면 더 이상 중앙 집중식 관리의 이점을 누릴 수 없으며 로컬 CLI 및 스크립트를 사용하여 어플라이언스를 관리해야 합니다.

STEP 1 | **Panorama** > 관리형 **WildFire** 어플라이언스를 선택합니다.

STEP 2 | 각 어플라이언스 옆의 체크박스를 선택하거나 어플라이언스 행을 클릭하여 Panorama 관리에서 제거하려는 WildFire 어플라이언스를 선택합니다.

STEP 3 | Panorama 관리에서 선택한 WildFire 어플라이언스를 제거합니다.

©2024 Palo Alto Networks, Inc.

WildFire 클러스터 관리

WildFire 어플라이언스 클러스터는 리소스를 풀링하여 샘플 분석 및 저장 용량을 늘리고 더 큰 방화벽 그룹을 지원하며 여러 WildFire 어플라이언스의 구성 및 관리를 단순화하는 상호 연결된 WildFire 어플라이언스 그룹입니다. 보안을 강화하고 전송된 콘텐츠의 기밀성을 유지하기 위해 클러스터의 WildFire 어플라이언스 간의 통신을 암호화할 수도 있습니다. WildFire 클러스터 및 배포 프로세스에 대한 자세한 내용은 WildFire 어플라이언스 클러스터를 참조하십시오.

Panorama를 사용하여 다음 작업을 수행하여 WildFire 클러스터를 관리할 수 있습니다.

- Panorama에서 중앙 집중식으로 클러스터 구성
- Panorama를 사용하여 WildFire 클러스터 상태 보기
- Panorama에서 중앙 집중식으로 사전 정의된 인증서를 사용하여 어플라이언스 간 암호화 구성
- Panorama에서 중앙 집중식으로 사용자 지정 인증서를 사용하여 어플라이언스 간 암호화 구성

Panorama에서 중앙 집중식으로 클러스터 구성

Panorama M-시리즈 또는 가상 어플라이언스에서 WildFire 어플라이언스 클러스터를 구성하기 전에 고가용성 컨트롤러 노드 쌍으로 구성할 수 있는 두 개의 WildFire 어플라이언스와 작업자 노드 역할을 하여 분석, 스토리지 용량, 클러스터의 탄력성.

WildFire 어플라이언스가 새 제품인 경우 WildFire 시작하기를 선택하여 WildFire 라이선스 활성화 확인, 로깅 활성화, WildFire 어플라이언스에 방화벽 연결, 기본 WildFire 기능 구성과 같은 기본 단계를 완료했는지 확인하십시오.

WildFire 어플라이언스 클러스터를 생성하려면 클러스터에 배치하려는 모든 WildFire 어플라이언스를 PAN-OS 8.0.1 이상으로 업그레이드해야 합니다. *Panorama*를 사용하여 *WildFire* 어플라이언스 클러스터를 관리하는 경우 *Panorama*는 *PAN-OS 8.0.1* 이상도 실행해야 합니다. 클러스터에 추가하려는 각 *WildFire* 어플라이언스에서 ***show system info*** | 어플라이언스가 *PAN-OS 8.0.1* 이상의 버전을 실행하고 있는지 확인하려면 *WildFire* 어플라이언스 *CLI*에서 버전을 일치시키십시오. 클러스터*(*또는 독립 실행형 어플라이언스*)*를 관리하는 데 사용하는 각 *Panorama* 어플라이언스에서 ***Dashboard*** > 일반 정보 > 소프트웨어 버전은 실행 중인 소프트웨어 버전을 표시합니다.

WildFire 어플라이언스를 사용할 수 있는 경우 적절한 작업을 수행합니다.

- 클러스터 구성 및 Panorama에 노드 추가
- Panorama에서 일반 클러스터 설정 구성
- WildFire 클러스터에 대한 인증 구성
- Panorama Management에서 클러스터 제거

*Panorama*를 사용하여 클러스터에서 노드를 제거하는 것은 지원되지 않습니다. 대신 로컬 WildFire CLI를 사용하여 클러스터에서 노드를 로컬로 제거하십시오.

 ©2024 Palo Alto Networks, Inc.

클러스터 구성 및 Panorama에 노드 추가

Panorama에서 WildFire 어플라이언스 클러스터를 구성하기 전에 Panorama를 8.0.1 이상으로 업그레이드하고 클러스터에 추가하려는 모든 WildFire 어플라이언스를 8.0.1 이상으로 업그레이드해야 합니다. 모든 WildFire 어플라이언스는 동일한 버전의 PAN-OS를 실행해야 합니다.

Panorama M-시리즈 또는 가상 어플라이언스로 최대 200개의 WildFire 어플라이언스를 관리할 수 있습니다. 200개의 WildFire 어플라이언스 제한은 독립 실행형 어플라이언스와 WildFire 어플라이언스 클러스터 노드의 합계입니다(Panorama로 관리할 독립 실행형 WildFire 어플라이언스도 추가하는 경우). 명시된 경우를 제외하고 구성은 Panorama에서 수행됩니다.

각 *WildFire* 어플라이언스 클러스터 노드에는 동일한 서브넷에 고정 *IP* 주소가 있어야 하고 연결 대기 시간이 짧아야 합니다.

STEP 1 | 로컬 CLI를 사용하여 WildFire 어플라이언스 클러스터를 관리할 Panorama 서버의 IP 주소를 구성합니다.

클러스터 또는 독립 실행형 WildFire 어플라이언스를 Panorama 어플라이언스에 등록하기 전에 먼저 로컬 WildFire CLI를 사용하여 각 WildFire 어플라이언스에서 Panorama IP 주소 또는 FQDN을 구성해야 합니다. 이것이 각 WildFire 어플라이언스가 어떤 Panorama 어플라이언스를 관리하는지 파악하는 방법입니다.

1. 각 WildFire 어플라이언스에서 기본 Panorama 어플라이언스 관리 인터페이스의 IP 주소 또는 FQDN을 구성합니다.

   ```
   admin@WF-500# set deviceconfig system panorama-server <ip-address | FQDN>
   ```

2. 각 WildFire 어플라이언스에서 고가용성을 위해 백업 Panorama 어플라이언스를 사용하는 경우(권장), 백업 Panorama 어플라이언스 관리 인터페이스의 IP 주소 또는 FQDN을 구성합니다.

   ```
   admin@WF-500# set deviceconfig system panorama-server-2 <ip-address | FQDN>
   ```

3. 각 WildFire 어플라이언스에서 구성을 커밋합니다.

   ```
   admin@WF-500# commit
   ```


©2024 Palo Alto Networks, Inc.

STEP 2 | 기본 Panorama 어플라이언스에서 WildFire 어플라이언스를 등록합니다.

새로 등록된 기기는 로컬 클러스터 구성으로 인해 이미 클러스터에 속해 있지 않는 한 독립형 모드입니다.

1. **Panorama** > **Managed WildFire** 어플라이언스를 선택하고 어플라이언스 추가를 선택합니다.
2. 별도의 줄에 각 WildFire 어플라이언스의 일련번호를 입력합니다. WildFire 어플라이언스 일련번호 목록이 없는 경우 로컬 CLI를 사용하여 각 WildFire 어플라이언스에서 **`show system info`**를 실행하여 일련번호를 얻습니다.
3. 확인을 클릭합니다.

   사용 가능한 경우 IP 주소 및 소프트웨어 버전과 같이 WildFire 어플라이언스에서 이미 커밋된 구성에 대한 정보가 표시됩니다. 이미 클러스터에 속한 WildFire 어플라이언스(예: 로컬 클러스터 구성으로 인해)는 클러스터 정보 및 연결 상태를 표시합니다.

STEP 3 | (선택 사항) WildFire 어플라이언스 구성을 Panorama 어플라이언스로 가져옵니다.

구성을 가져오면 Panorama에서 구성을 재사용하거나 편집한 다음 하나 이상의 WildFire 어플라이언스 클러스터 또는 독립형 WildFire 어플라이언스에 푸시할 수 있으므로 시간이 절약됩니다. 가져올 구성이 없으면 이 단계를 건너뜁니다. Panorama에서 구성을 푸시하면 푸시된 구성이 로컬 구성을 덮어씁니다.

1. **Panorama** > 관리형 **WildFire Appliances**를 선택하고 관리되는 WildFire 어플라이언스 목록에서 가져오려는 구성이 있는 어플라이언스를 선택합니다.
2. 구성을 가져옵니다.
3. 예를 선택합니다.

   구성을 가져오면 표시된 정보가 업데이트되고 가져온 구성이 Panorama 어플라이언스 후보 구성의 일부가 됩니다.
4. 불러온 WildFire 어플라이언스 구성을 Panorama 실행 구성의 일부로 만들려면 **Panorama**에 커밋합니다.

STEP 4 | 새 WildFire 어플라이언스 클러스터를 생성합니다.

1. 관리형 **WildFire** 클러스터를 선택합니다.

   어플라이언스 > 할당된 클러스터 없음은 독립형 WildFire 어플라이언스(노드)를 표시하고 클러스터에 할당되지 않은 사용 가능한 노드 수를 나타냅니다.
2. 클러스터를 생성합니다.
3. 최대 63자의 영숫자 클러스터 이름을 입력하십시오. 이름에는 소문자와 숫자가 포함될 수 있으며, 첫 번째 또는 마지막 문자가 아닌 경우 하이픈과 마침표가 포함될 수 있습니다. 공백이나 다른 문자는 허용되지 않습니다.
4. 확인을 클릭합니다.

   새 클러스터 이름이 표시되지만 할당된 WildFire 노드가 없습니다.

STEP 5 | 새 클러스터에 WildFire 어플라이언스를 추가합니다.

클러스터에 추가된 첫 번째 WildFire 어플라이언스는 자동으로 컨트롤러 노드가 되고 클러스터에 추가된 두 번째 WildFire 어플라이언스는 자동으로 컨트롤러 백업 노드가 됩니다. 클러스터에 추가된 모든

 ©2024 Palo Alto Networks, Inc.

후속 WildFire 어플라이언스는 작업자 노드가 됩니다. 작업자 노드는 클러스터가 일관된 구성을 갖도록 컨트롤러 노드 설정을 사용합니다.

1. 새 클러스터를 선택합니다.
2. 클러스터링을 선택합니다.
3. 클러스터에 속하지 않은 WildFire 어플라이언스 목록을 찾습니다.
4. 클러스터에 포함할 각 WildFire 어플라이언스를 추가(⊕)합니다. 클러스터에 최대 20개의 노드를 추가할 수 있습니다. 클러스터에 추가하는 각 WildFire 어플라이언스는 자동으로 할당된 역할과 함께 표시됩니다.
5. 확인을 클릭합니다.

©2024 Palo Alto Networks, Inc.

STEP 6 | 관리, 분석 환경 네트워크, HA 및 클러스터 관리 인터페이스를 구성합니다.

아직 구성되지 않은 경우 각 클러스터 구성원(컨트롤러 및 작업자 노드)에서 관리, 분석 환경 네트워크 및 클러스터 관리 인터페이스를 구성하십시오. 클러스터 관리 인터페이스는 클러스터 내에서 관리 및 통신을 위한 전용 인터페이스이며 관리 인터페이스와 동일하지 않습니다.

컨트롤러 노드와 컨트롤러 백업 노드 모두에서 HA 인터페이스를 개별적으로 구성합니다. HA 인터페이스는 기본 및 백업 컨트롤러 노드를 연결하고 동기화 상태를 유지하고 페일오버에 응답할 수 있도록 합니다.

클러스터 노드에는 *4*개의 *WildFire* 어플라이언스 인터페이스 각각에 대한 *IP* 주소가 필요합니다. 작업자 노드에서는 *HA* 서비스를 구성할 수 없습니다.

1. 새 클러스터를 선택합니다.
2. 클러스터링을 선택합니다.
3. 클러스터 노드에 관리 인터페이스가 구성되지 않은 경우 인터페이스 이름 > 관리를 선택하고 인터페이스에 대한 IP 주소, 넷마스크, 서비스 및 기타 정보를 입력합니다.
4. Analysis Environment Network에 대한 인터페이스가 클러스터 노드에 구성되지 않은 경우 인터페이스 이름 > 분석 환경 네트워크를 선택하고 인터페이스에 대한 IP 주소, 넷마스크, 서비스 및 기타 정보를 입력합니다.
5. 컨트롤러 노드와 컨트롤러 백업 노드 모두에서 HA 제어 링크에 사용할 인터페이스를 선택합니다. HA 서비스에 대해 두 컨트롤러 노드에서 동일한 인터페이스를 구성해야 합니다. 예를 들어, 컨트롤러 노드에서 컨트롤러 백업 노드에서 **Ethernet3**을 선택합니다.
6. 각 컨트롤러 노드에 대해 클러스터링 서비스 > **HA**를 선택합니다. (워커 노드에는 **HA** 옵션을 사용할 수 없습니다.) 인터페이스를 ping하는 기능도 원하는 경우 관리 서비스 > **Ping**.
7. 확인을 클릭합니다.
8. (권장) 컨트롤러 노드와 컨트롤러 백업 노드 간의 백업 HA 제어 링크로 사용할 인터페이스를 선택합니다. HA 백업 서비스를 위해 두 노드에서 동일한 인터페이스를 사용해야 합니다. 예를 들어 두 노드 모두에서 관리를 선택합니다.

   두 노드 모두에 대해 **Clustering Services** > **HA** 백업을 선택합니다. 인터페이스에서 해당 관리 서비스를 원하는 경우 **Ping**, **SSH** 및 **SNMP**를 선택할 수도 있습니다.

   Analysis Environment 네트워크 인터페이스는 *HA* 또는 *HA* 백업 인터페이스 또는 클러스터 관리 인터페이스가 될 수 없습니다.
9. 클러스터 내에서 관리 및 통신에 사용할 전용 인터페이스를 선택합니다. 두 노드에서 동일한 인터페이스(예: **Ethernet2**)를 사용해야 합니다.
10. 두 노드에 대해 클러스터링 서비스 > 클러스터 관리를 선택합니다. 인터페이스에 대한 핑(ping) 기능도 원하는 경우 관리 서비스 > **Ping**을 선택합니다.

    클러스터의 작업자 노드는 전용 관리 및 통신 인터페이스에 대한 컨트롤러 노드의 설정을 자동으로 상속합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama 어플라이언스에서 구성을 커밋하고 클러스터에 푸시합니다.

1. 커밋하고 푸시합니다.
2. Panorama 어플라이언스에 푸시하지 않으려는 구성이 있는 경우 선택 편집을 클릭하여 구성을 푸시할 어플라이언스를 선택합니다. 푸시된 구성은 모든 클러스터 노드가 동일한 구성을 실행하도록 클러스터 노드에서 실행 중인 구성을 덮어씁니다.

STEP 8 | 구성을 확인합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택합니다.
2. 다음 필드를 확인하십시오.
   - 기기 - 독립 실행형 기기로 표시되는 대신 클러스터에 추가된 WildFire 노드가 클러스터 이름 아래에 표시됩니다.
   - 클러스터 이름 - 각 노드에 대해 클러스터 이름이 표시됩니다.
   - 역할 - 각 노드에 대해 적절한 역할(컨트롤러, 컨트롤러 백업 또는 작업자)이 표시됩니다.
   - 구성 상태 - 상태가 `InSync`입니다.
   - 마지막 커밋 상태 - ####.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 기본 컨트롤러 노드(Panorama 웹 인터페이스 아님)에서 로컬 CLI를 사용하여 구성이 동기화되었는지 확인합니다.

동기화되지 않은 경우 컨트롤러 노드에서 고가용성 구성을 수동으로 동기화하고 구성을 커밋합니다.

Panorama에서 대부분의 다른 구성을 수행할 수 있지만 컨트롤러 노드 고가용성 구성 동기화는 기본 컨트롤러 노드의 CLI에서 수행해야 합니다.

1. 기본 컨트롤러 노드에서 구성이 동기화되었는지 확인합니다.

   ```
   admin@WF-500(active-controller)> show high-availability all
   ```

   출력 끝에서 `ConfigurationSynchronization` 출력을 찾습니다.

   ```
   ## ###: ####: # ## ## ##: ####
   ```

   실행 중인 구성이 동기화되면 구성을 수동으로 동기화할 필요가 없습니다. 그러나 구성이 동기화되지 않은 경우 구성을 수동으로 동기화해야 합니다.
2. 구성이 동기화되지 않은 경우 기본 컨트롤러 노드에서 고가용성 구성을 원격 피어 컨트롤러 노드와 동기화합니다.

   ```
   admin@WF-500(active-controller)> request high-availability
    sync-to-remote running-config
   ```

   기본 컨트롤러 노드의 구성과 컨트롤러 백업 노드의 구성이 일치하지 않는 경우 기본 컨트롤러 노드의 구성이 컨트롤러 백업 노드의 구성을 재정의합니다.
3. 구성 커밋:

   ```
   admin@WF-500# commit
   ```

Panorama에서 일반 클러스터 설정 구성

일부 일반 설정은 선택 사항이며 일부 일반 설정은 기본값으로 미리 채워져 있습니다. 클러스터 구성이 요구 사항과 일치하는지 확인하려면 최소한 이러한 설정을 확인하는 것이 가장 좋습니다. 일반 설정에는 다음이 포함됩니다.

- WildFire 퍼블릭 클라우드에 연결하고 샘플을 퍼블릭 클라우드에 제출합니다.
- 데이터 보존 정책 구성.
- 로깅 구성.
- 분석 환경(사용자 환경과 가장 일치하는 VM 이미지)을 설정하고 방화벽이 WildFire에 제출하는 샘플 유형을 가장 잘 서비스하도록 분석 환경을 사용자 지정합니다.
- DNS 서버, NTP 서버 등에 대한 IP 주소를 설정합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | WildFire 어플라이언스 클러스터 노드에 대한 설정을 구성합니다.

많은 설정이 기본값, 컨트롤러 노드의 이전 기존 설정 정보 또는 방금 구성한 설정으로 미리 채워져 있습니다.

1. 클러스터를 선택합니다.
2. 기기를 선택합니다.
3. 새 정보를 입력하거나 클러스터 컨트롤러 노드에서 미리 채워진 정보를 유지하거나 다음을 포함하여 미리 채워진 정보를 편집합니다.
   - 도메인 이름.
   - 기본 **DNS** 서버 및 보조 **DNS** 서버의 IP 주소입니다.
   - 기본 **NTP** 서버 및 보조 **NTP** 서버의 **NTP** 서버 주소 및 인증 유형입니다. 인증 유형 옵션은 없음, 대칭 키 및 자동 키입니다.

STEP 2 | 일반 클러스터 설정을 구성합니다.

많은 설정이 기본값, 컨트롤러 노드의 이전 기존 설정 정보 또는 방금 구성한 설정으로 미리 채워져 있습니다.

1. 새 클러스터 > 일반을 선택하십시오.
2. (선택 사항) 컨트롤러 노드가 DNS 프로토콜을 사용하여 서비스 상태를 알리도록 **DNS**를 활성화합니다. 클러스터 컨트롤러는 관리(MGT) 인터페이스 포트에서 DNS 서비스를 제공합니다.
3. 방화벽 등록 클러스터 컨트롤러에서 보급한 서비스를 사용합니다. Palo Alto Networks는 고가용성의 이점을 제공하기 때문에 두 컨트롤러를 모두 권한 서버로 추가할 것을 권장합니다. 다음 형식을 사용합니다.

   ```
   wfpc.service.<cluster-name>.<domain>
   ```

   예를 들어 *paloaltonetworks.com* 도메인에 있는 *mycluster*라는 클러스터의 도메인 이름은 다음과 같습니다.

   ```
   wfpc.service.mycluster.paloaltonetworks.com
   ```

4. 클러스터에 대한 콘텐츠 업데이트 서버를 입력합니다. 기본 `updates.paloaltonetworks.com` FQDN을 사용하여 가장 가까운 서버에 연결합니다. 서버 **ID**를 확인하여 인증서의 CN(일반 이름)을 서버의 IP 주소 또는 FQDN과 일치시켜 업데이트 서버 ID를 확인합니다(기본적으로 선택됨).
5. (선택 사항) 클러스터(또는 Panorama에서 관리하는 독립 실행형 어플라이언스)가 가장 가까운 WildFire 클라우드 서버에 정보를 보낼 수 있도록 공용 **WildFire** 클라우드 서버 위치를 입력하거나 기본 `wildfire.paloaltonetworks.com`을 사용합니다. 이 필드를 비워두고 WildFire 클라우드 서버에 연결하지 않으면 클러스터는 WildFire 퍼블릭 클라우드에서 직접 서

 ©2024 Palo Alto Networks, Inc.

명 업데이트를 수신할 수 없으며 분석을 위해 샘플을 보내거나 퍼블릭 클라우드에 데이터를 제공할 수 없습니다.

6. 클러스터를 공용 WildFire 클라우드에 연결하는 경우 활성화할 클라우드 서비스를 선택합니다.
   - 분석 데이터 보내기 - 로컬 맬웨어 분석에 대한 XML 보고서를 보냅니다. 실제 샘플을 보내면 클러스터는 보고서를 보내지 않습니다.
   - 악성 샘플 보내기 - 멀웨어 샘플을 보냅니다.
   - 진단 보내기 - 진단 데이터를 보냅니다.
   - 판정 조회 - 로컬 WildFire 어플라이언스 클러스터의 부하를 줄이기 위해 로컬 분석을 수행하기 전에 판정에 대해 WildFire 퍼블릭 클라우드를 자동으로 쿼리합니다.
7. 클러스터에서 분석할 샘플 유형에 따라 사용할 샘플 분석 이미지를 선택합니다.
8. 클러스터가 **Benign/Grayware** 샘플 데이터(1-90일 범위, 기본 14일) 및 악성 샘플 데이터(최소 1일, 최대 없음(무한), 기본값은 무기한)를 유지하는 시간을 구성합니다. 악성 샘플 데이터에는 피싱 판정이 포함됩니다.
9. (선택 사항) 기본 분석 환경을 선택하여 환경에 따라 실행 파일 또는 문서에 더 많은 리소스를 할당합니다. 기본 할당은 실행 파일과 문서 간에 균형을 이룹니다. 사용 가능한 리소스 양은 클러스터의 WildFire 노드 수에 따라 다릅니다.

STEP 3 | 기본 및 백업 Panorama 서버가 구성되어 있는지 확인하십시오.

백업 Panorama 서버를 구성하지 않았고 구성하려는 경우 백업 Panorama 서버를 추가할 수 있습니다.

1. 클러스터를 선택합니다.
2. 기기를 선택합니다.
3. 중앙 집중식 클러스터 관리를 위해 고가용성 구성을 사용하는 경우 기본 **Panorama Server** 및 백업 **Panorama Server 2**의 IP 주소 또는 FQDN을 확인(또는 입력)하십시오.

STEP 4 | (선택 사항) 로그 포워딩을 포함하여 클러스터에 대한 시스템 및 구성 로그 설정을 구성합니다.

1. 클러스터를 선택합니다.
2. 로깅을 선택합니다.
3. 시스템 또는 구성을 선택하여 각각 시스템 또는 구성 로그를 구성합니다. 구성 프로세스는 유사합니다.
4. 추가(⊕) 및 로그 포워딩 인스턴스의 이름을 지정하고 필터를 선택한 다음 포워딩 메서드(**SNMP**, 이메일, **Syslog** 또는 **HTTP**)을 구성합니다.

STEP 5 | 관리자 인증을 구성합니다.

1. 클러스터를 선택합니다.
2. 인증을 선택합니다.
3. 없음 또는 반경에서 인증 프로파일을 선택합니다. RADIUS는 유일하게 지원되는 외부 인증 방법입니다.
4. 관리자 사용자의 로컬 인증 모드를 암호 또는 암호 해시로 설정하고 암호를 입력합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | Panorama 어플라이언스에서 구성을 커밋하고 클러스터에 푸시합니다.

1. 커밋하고 푸시합니다.
2. Panorama 어플라이언스에 푸시하지 않으려는 구성이 있는 경우 선택 편집을 클릭하여 구성을 푸시할 어플라이언스를 선택합니다. 푸시된 구성은 모든 클러스터 노드가 동일한 구성을 실행하도록 클러스터 노드에서 실행 중인 구성을 덮어씁니다.

WildFire 클러스터에 대한 인증 구성

세분화된 인증 매개변수를 사용하여 로컬 관리 사용자를 구성하고 권한 부여 및 인증을 위해 RADIUS, TACAS+ 또는 LDAP를 활용하여 WildFire 클러스터의 모든 WildFire 어플라이언스에 대한 향상된 인증을 생성 및 구성합니다.

Panorama에서 관리자를 구성하고 푸시하면 WildFire 클러스터의 모든 WildFire 어플라이언스에 대한 기존 관리자를 Panorama에서 구성한 관리자로 덮어씁니다.

- WildFire 클러스터에 대한 관리 계정 구성
- WildFire 클러스터에 대한 RADIUS 인증 구성
- WildFire 클러스터에 대한 TACACS+ 인증 구성
- WildFire 클러스터에 대한 LDAP 인증 구성

WildFire 클러스터에 대한 관리 계정 구성

Panorama™ 관리 서버에서 관리할 WildFire 클러스터의 모든 WildFire 어플라이언스에 대한 세분화된 인증 매개변수를 사용하여 한 명 이상의 관리자를 생성합니다. 또한 WildFire 어플라이언스의 CLI에서 직접 구성할 수 있는 Panorama에서 로컬 관리자를 구성할 수 있습니다. 그러나 WildFire 어플라이언스에 새 구성 변경 사항을 푸시하면 WildFire 어플라이언스에 대해 구성된 관리자가 로컬 관리자를 덮어씁니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama에서 중앙 집중식으로 클러스터 구성.

STEP 3 | (선택 사항) WildFire 어플라이언스 CLI에 액세스하는 관리자의 로그인 자격 증명을 확인하는 인증 서비스를 정의하도록 인증 프로파일을 구성합니다.

STEP 4 | 필요에 따라 하나 이상의 관리자 계정을 구성합니다.

Panorama에서 생성된 관리자 계정은 나중에 WildFire 클러스터의 WildFire 어플라이언스로 가져와 Panorama에서 관리됩니다.

WildFire 클러스터에서 *Wildfire* 어플라이언스에 대한 인증을 성공적으로 구성하려면 운용 관리자 역할 권한이 있는 관리 계정을 구성해야 합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | WildFire 클러스터에서 WildFire 어플라이언스에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 이전에 구성한 WildFire 클러스터를 선택합니다.
2. (선택 사항) 이전 단계에서 구성한 인증 프로파일을 선택합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

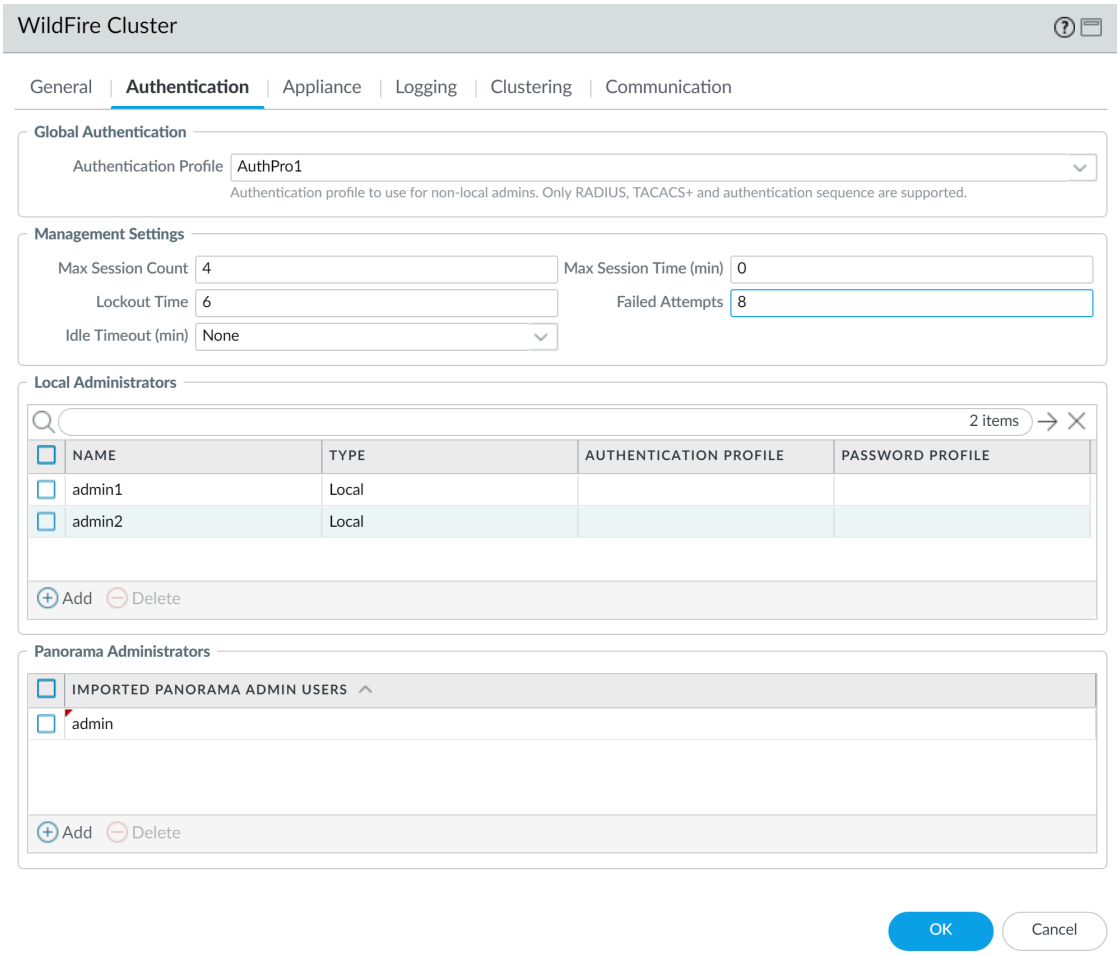
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 클러스터의 WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 해당 관리자가 생성된 WildFire 클러스터의 WildFire 어플라이언스에만 해당되며 사용자는 이 표에서 이러한 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 WildFire 클러스터의 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 클러스터 인증 구성을 저장합니다.



STEP 6 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 7 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 클러스터에 대한 RADIUS 인증 구성

RADIUS 서버를 사용하여 WildFire 클러스터에 있는 WildFire 어플라이언스의 CLI에 대한 관리 액세스를 인증합니다. RADIUS 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹

 ©2024 Palo Alto Networks, Inc.

을 신속하게 변경할 수 있습니다. 이는 Panorama™ 관리 서버에서 설정을 재구성하는 것보다 훨씬 쉽습니다.



Palo Alto Networks RADIUS 사전을 *RADIUS* 서버로 가져와 *Panorama*와 *RADIUS* 서버 간의 통신에 필요한 인증 속성을 정의할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama에서 중앙 집중식으로 클러스터 구성.

©2024 Palo Alto Networks, Inc.

STEP 3 | RADIUS 인증을 구성합니다.

WildFire 클러스터에서 *Wildfire* 어플라이언스에 대한 인증을 성공적으로 구성하려면 *RADIUS* 인증을 위해 구성된 관리자 계정에 운용 관리자 역할 권한이 있어야 합니다.

1. RADIUS 서버 프로파일을 추가합니다.

   프로파일은 WildFire 클러스터의 WildFire 어플라이언스가 RADIUS 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server** 프로파일 > **RADIUS**를 선택하고 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 1–20 범위).
   4. WildFire 어플라이언스가 RADIUS 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.

      RADIUS 서버가 해당 프로토콜을 지원하는 경우 ***CHAP***를 선택하십시오. ***PAP***보다 더 안전합니다.

   5. 각 RADIUS 서버를 추가하고
      1. 서버를 식별할 이름을 입력합니다.
      2. **RADIUS** 서버 IP 주소 또는 FQDN.
      3. 암호/암호 확인(사용자 이름과 암호를 암호화하는 키)
      4. 인증 요청을 위한 서버 포트(기본값은 1812).
   6. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. RADIUS 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택하고 프로파일을 추가합니다.
   2. 인증 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **RADIUS**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. **RADIUS**에서 사용자 그룹 검색을 선택하여 RADIUS 서버에 정의된 VSA에서 사용자 그룹 정보를 수집합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.

   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 클러스터에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 이전에 추가한 WildFire 클러스터를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

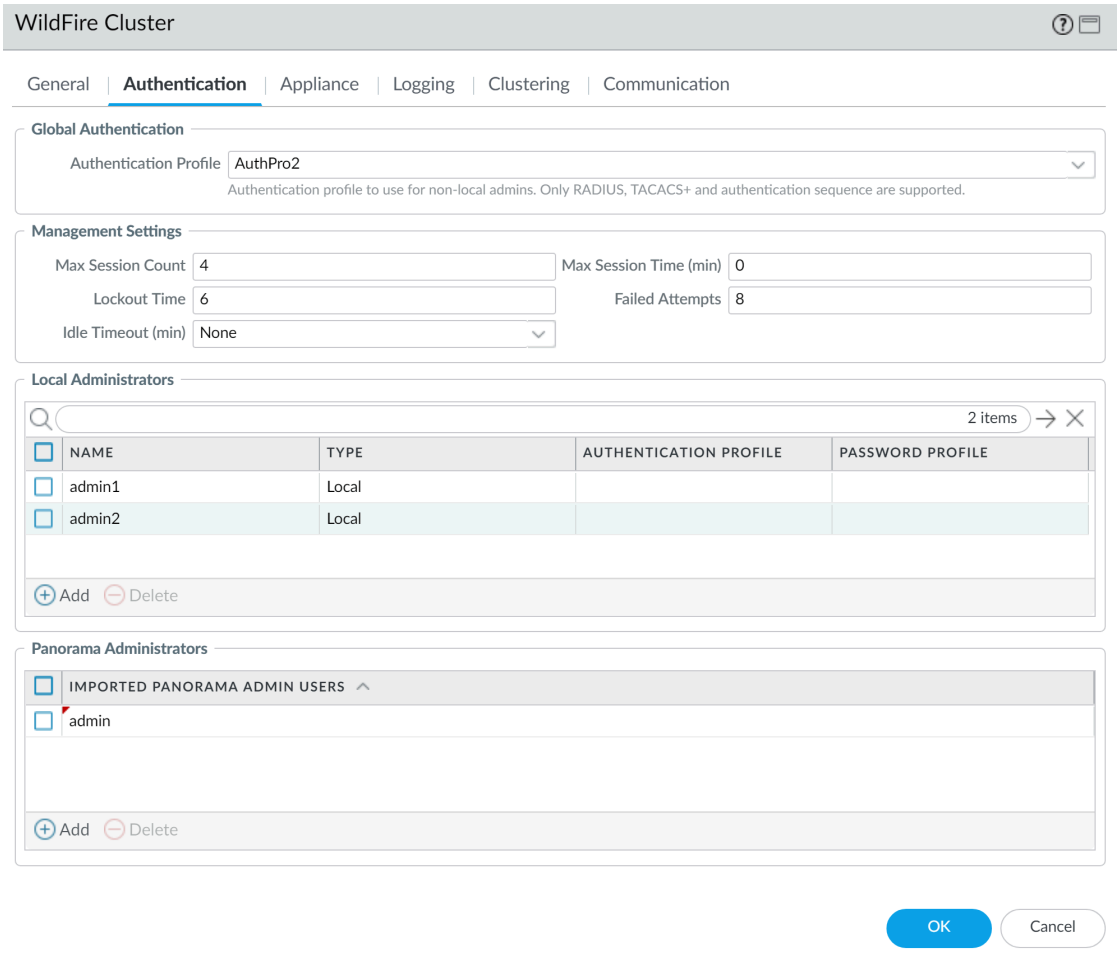
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 클러스터의 WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 해당 관리자가 생성된 WildFire 클러스터의 WildFire 어플라이언스에만 해당되며 사용자는 이 표에서 이러한 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 WildFire 클러스터의 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 클러스터 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 클러스터에 대한 TACACS+ 인증 구성

TACACS+ 서버를 사용하여 WildFire 클러스터에 있는 WildFire 어플라이언스의 CLI에 대한 관리 액세스를 인증할 수 있습니다. TACACS+ 서버에서 VSA(Vendor-Specific Attributes)를 정의하여 관리자 권한 부여를 관리할 수도 있습니다. VSA를 사용하면 디렉토리 서비스를 통해 관리자의 역할, 액세스 도메인 및 사용자 그룹을 신속하게 변경할 수 있습니다. 이는 Panorama에서 설정을 재구성하는 것보다 쉬운 경우가 많습니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama에서 중앙 집중식으로 클러스터 구성.

STEP 3 | TACACS+ 인증을 구성합니다.

WildFire 클러스터에서 *Wildfire* 어플라이언스에 대한 인증을 성공적으로 구성하려면 *TACACS+* 인증을 위해 구성된 관리자 계정에 운용 관리자 관리 역할 권한이 있어야 합니다.

1. TACACS+ 서버 프로파일을 추가합니다.

   프로파일은 WildFire 어플라이언스가 TACACS+ 서버에 연결하는 방법을 정의합니다.

   1. **Panorama** > **Server Profiles** > **TACACS+**를 선택한 다음 프로파일을 추가합니다.
   2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
   3. 인증 요청 시간이 초과되는 타임아웃 간격(초)을 입력합니다(기본값은 3, 범위는 1–20).
   4. Panorama가 TACACS+ 서버에 인증하는 데 사용하는 인증 프로토콜(기본값은 **CHAP**)을 선택합니다.
   5. TACACS+ 서버가 해당 프로토콜을 지원하는 경우 **CHAP**를 선택하십시오. **PAP**보다 더 안전합니다.
   6. 각 TACACS+ 서버를 추가하고 서버를 식별할
      1. 이름을 입력합니다.
      2. **TACACS+** 서버 IP 주소 또는 FQDN.
      3. 암호/암호 확인(사용자 이름과 암호를 암호화하는 키).
      4. 인증 요청을 위한 서버 포트(기본값은 49).
   7. 확인을 클릭하여 서버 프로파일을 저장합니다.
2. TACACS+ 서버 프로파일을 인증 프로파일에 할당합니다.

   인증 프로파일은 관리자 집합에 공통적인 인증 설정을 정의합니다.

   1. **Panorama** > 인증 프로파일을 선택한 다음 프로파일을 추가합니다.
   2. 프로파일을 식별할 이름을 입력합니다.
   3. 유형을 **TACACS+**로 설정합니다.
   4. 구성한 서버 프로파일을 선택합니다.
   5. TACACS+ 서버에 정의된 VSA에서 사용자 그룹 정보를 수집하려면 TACACS+에서 사용자 그룹 검색을 선택합니다.

      Panorama는 인증 프로파일의 허용 목록에서 지정한 그룹과 그룹 정보를 일치시킵니다.
   6. **Advanced**를 선택하고 허용 목록에서 이 인증 프로파일로 인증할 수 있는 관리자를 추가합니다.
   7. 확인을 클릭하여 인증 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 클러스터에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 이전에 추가한 WildFire 클러스터를 선택합니다.
2. 이전 단계에서 구성한 인증 프로파일을 선택합니다.

   전역 인증 프로파일이 할당되지 않은 경우 원격 인증을 활용하려면 각 개별 로컬 관리자에게 인증 프로파일을 할당해야 합니다.
3. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
4. WildFire 어플라이언스 관리자를 추가합니다.

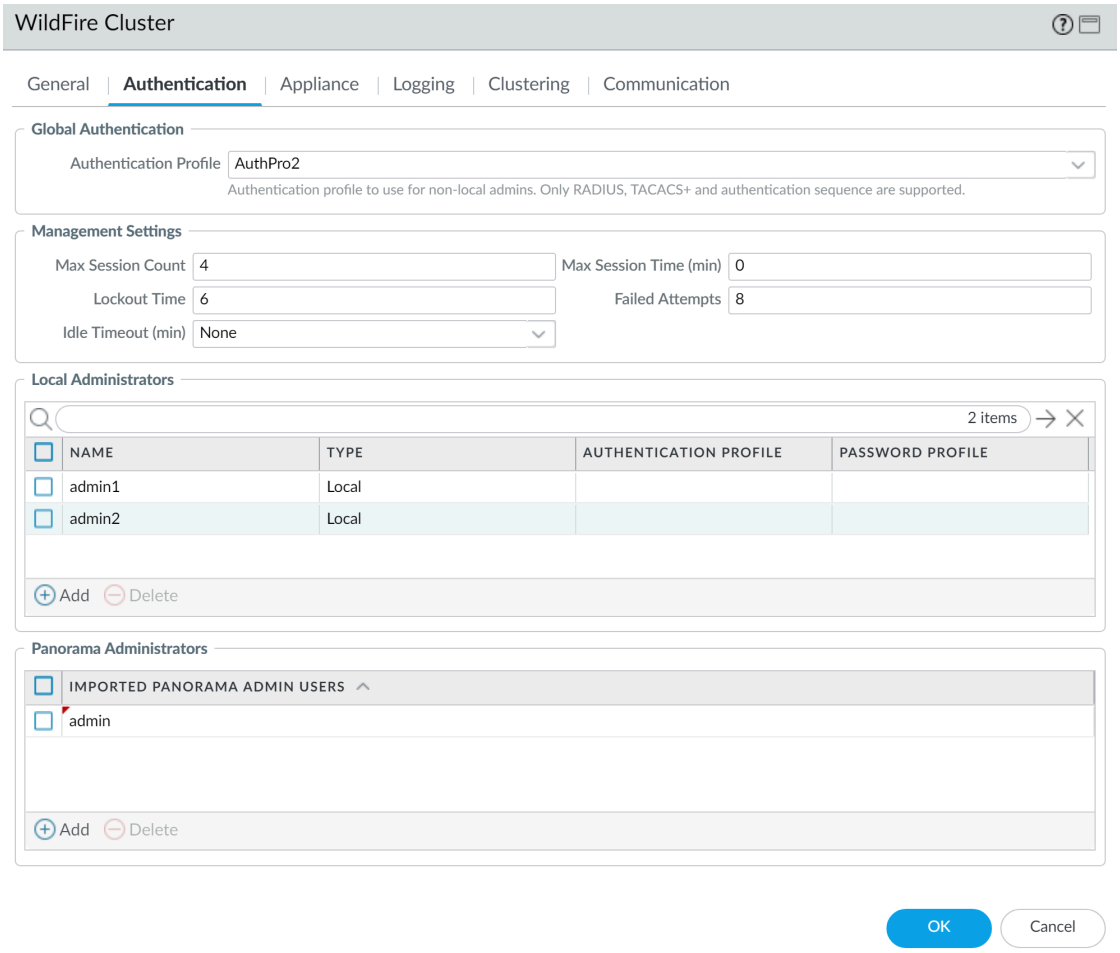
   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

1. WildFire 클러스터의 WildFire 어플라이언스에 고유한 새 관리자를 추가하고 구성합니다. 이러한 관리자는 해당 관리자가 생성된 WildFire 클러스터의 WildFire 어플라이언스에만 해당되며 사용자는 이 표에서 이러한 관리자를 관리합니다.
2. Panorama에 구성된 모든 관리자를 추가합니다. 이러한 관리자는 Panorama에서 생성되고 WildFire 클러스터의 WildFire 어플라이언스로 가져옵니다.

5. 확인을 클릭하여 WildFire 클러스터 인증 구성을 저장합니다.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

WildFire 클러스터에 대한 LDAP 인증 구성

LDAP를 사용하여 최종 사용자가 WildFire 클러스터에 있는 WildFire 어플라이언스의 CLI에 액세스하도록 인증할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에서 중앙 집중식으로 클러스터 구성.

STEP 3 | LDAP 서버 프로파일을 추가합니다.

프로파일은 WildFire 어플라이언스가 LDAP 서버에 연결하는 방법을 정의합니다.

WildFire 클러스터에서 *WildFire* 어플라이언스에 대한 인증을 성공적으로 구성하려면 *LDAP* 인증을 위해 구성된 관리자 계정에 운용 관리자 역할 권한이 있어야 합니다.

1. **Panorama** > 서버 프로파일 > **LDAP** 및 서버 프로파일 추가를 선택합니다.
2. 프로파일 이름을 입력하여 서버 프로파일을 식별합니다.
3. LDAP 서버를 추가합니다(최대 4개). 각 서버에 대해 이름(서버 식별), **LDAP** 서버 IP 주소 또는 FQDN 및 서버 포트(기본값 389)를 입력합니다.

   FQDN 주소 개체를 사용하여 서버를 식별하고 이후에 주소를 변경하는 경우 새 서버 주소에 대한 변경 사항을 적용해야 합니다.
4. 서버 유형을 선택합니다.
5. 기본 **DN**을 선택합니다.

   디렉터리의 기본 DN을 식별하려면 **Active Directory** 도메인 및 트러스트 Microsoft 관리 콘솔 스냅인을 열고 최상위 도메인의 이름을 사용합니다.
6. 바인딩 **DN** 및 암호를 입력하여 인증 서비스에서 방화벽을 인증할 수 있도록 합니다.

   Bind DN 계정에는 *LDAP* 디렉토리를 읽을 수 있는 권한이 있어야 합니다.
7. 바인딩 타임아웃 및 검색 타임아웃(초)을 입력합니다. 기본값은 모두 30입니다.
8. 재시도 간격(초)을 입력합니다(기본값은 60).
9. (선택 사항) 엔드포인트가 디렉터리 서버와의 보다 안전한 연결을 위해 SSL 또는 TLS를 사용하도록 하려면 **SSL/TLS** 보안 연결 필요(기본적으로 활성화됨) 옵션을 활성화합니다. 엔드포인트가 사용하는 프로토콜은 서버 포트에 따라 다릅니다.
   - 389(기본값) - TLS(특히 WildFire 어플라이언스는 StartTLS 작업을 사용하여 초기 일반 텍스트 연결을 TLS로 업그레이드합니다.)
   - 636—SSL
   - 기타 포트 - WildFire 어플라이언스는 먼저 TLS 사용을 시도합니다. 디렉토리 서버가 TLS를 지원하지 않는 경우 WildFire 어플라이언스는 SSL로 대체합니다.
10. (선택 사항) 보안을 강화하려면 SSL/TLS 연결에 대해 디렉터리 서버가 제공하는 인증서를 엔드포인트에서 확인할 수 있도록 **SSL** 세션에 대한 서버 인증서 확인 옵션을 활성화합니다. 확인을 활성화하려면 **SSL/TLS** 보안 연결 필요 옵션도 활성화해야 합니다. 확인이 성공하려면 인증서가 다음 조건 중 하나를 충족해야 합니다.
    - Panorama 인증서 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서 > 디바이스 인증서. 필요한 경우 인증서를 Panorama로 가져옵니다.
    - 인증서 서명자는 신뢰할 수 있는 인증 기관 목록에 있습니다. **Panorama** > 인증서 관리 > 인증서.
11. 확인을 클릭하여 서버 프로파일을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | WildFire 클러스터에 대한 인증을 구성합니다.

1. **Panorama** > 관리형 **WildFire** 클러스터를 선택하고 이전에 추가한 WildFire 클러스터를 선택합니다.
2. WildFire 어플라이언스에 대한 인증 타임아웃 구성을 구성합니다.
   1. 사용자가 WildFire 어플라이언스 CLI에서 잠기기 전에 실패한 시도 횟수를 입력합니다.
   2. 사용자가 구성된 실패한 시도 횟수에 도달한 후 WildFire 어플라이언스가 사용자 계정을 잠그는 잠금 시간(분)을 입력합니다.
   3. 사용자 계정이 비활성으로 인해 자동으로 로그아웃되기 전의 유휴 타임아웃(분)을 입력합니다.
   4. 최대 세션 수를 입력하여 WildFire 어플라이언스에 동시에 액세스할 수 있는 사용자 계정 수를 설정합니다.
   5. 관리자가 자동으로 로그아웃되기 전에 로그인할 수 있는 최대 세션 시간을 입력합니다.
3. WildFire 어플라이언스 관리자를 추가합니다.

   관리자는 로컬 관리자 또는 불러온 Panorama 관리자로 추가할 수 있지만 둘 다 추가할 수는 없습니다. 동일한 관리자를 로컬 관리자 및 불러온 Panorama 관리자로 추가하는 것은 지원되지 않

 ©2024 Palo Alto Networks, Inc.

으며 Panorama 커밋이 실패합니다. 예를 들어 **admin1**을 로컬 및 Panorama 관리자로 추가하면 Panorama에 대한 커밋이 실패합니다.

- 로컬 관리자를 구성합니다.

  WildFire 클러스터에서 WildFire 어플라이언스에 고유한 새 관리자를 구성합니다 이러한 관리자는 해당 관리자가 생성된 WildFire 클러스터의 WildFire 어플라이언스에만 해당되며 사용자는 이 표에서 이러한 관리자를 관리합니다.

  1. 한 명 이상의 새 로컬 관리자를 추가하십시오.
  2. 로컬 관리자의 이름을 입력합니다.
  3. 이전에 생성한 인증 프로파일을 할당합니다.

     LDAP 인증 프로파일은 개별 로컬 관리자에 대해서만 지원됩니다.

  4. 인증을 위해 공개 키 파일을 가져오려면 공개 키 인증**(SSH)** 사용을 활성화(선택)합니다.
  5. 암호 프로파일을 선택하여 만료 매개변수를 설정합니다.

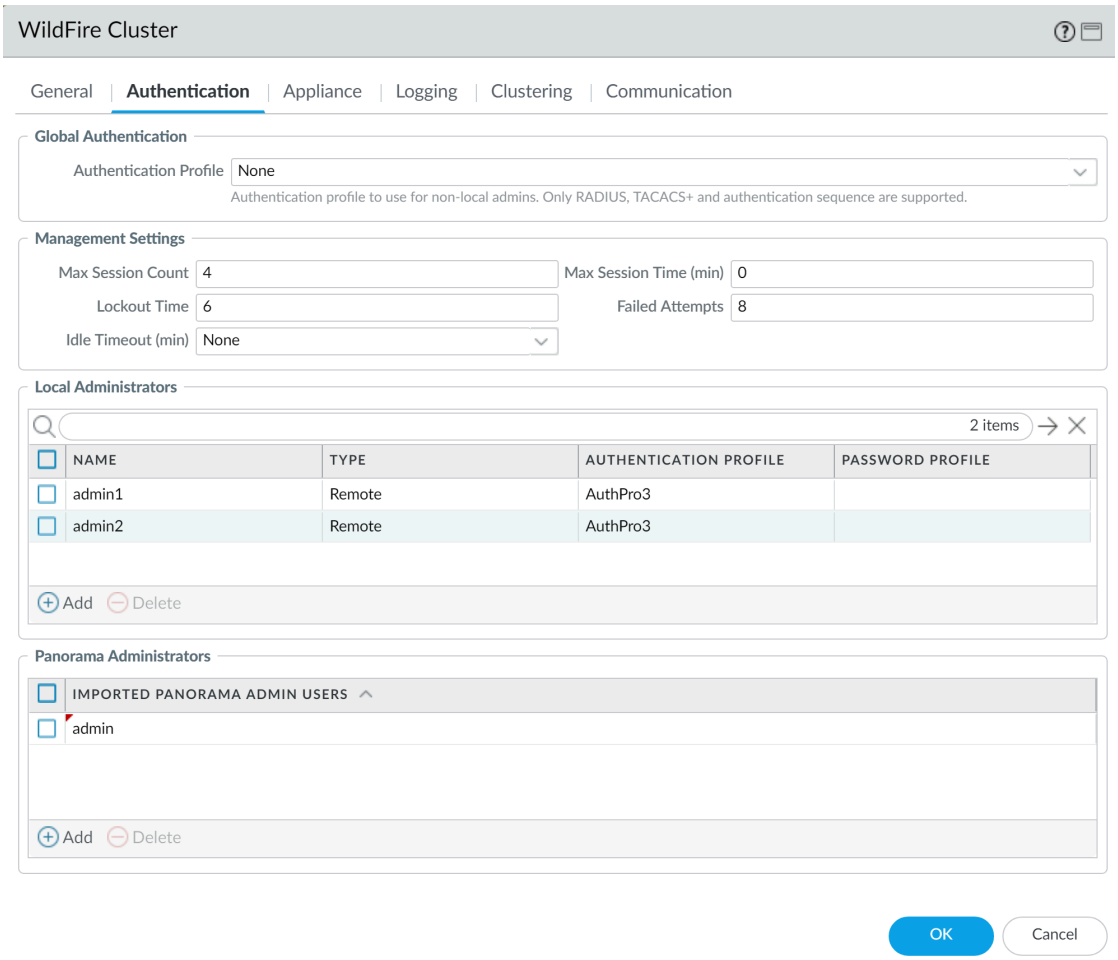
- 기존 Panorama 관리자 가져오기

  Panorama에 구성된 기존 관리자를 가져옵니다. 이러한 관리자는 Panorama에서 구성 및 관리되며 WildFire 클러스터의 모든 WildFire 어플라이언스로 가져옵니다.

  1. 기존 Panorama 관리자 추가

4. 확인을 클릭하여 WildFire 클러스터 인증 구성을 저장합니다.

 ©2024 Palo Alto Networks, Inc.



STEP 5 | 커밋한 다음 구성 변경 사항을 커밋하고 푸시합니다.

STEP 6 | WildFire 어플라이언스 CLI에 액세스하여 로컬 관리자를 사용하여 WildFire 어플라이언스에 성공적으로 액세스할 수 있는지 확인합니다.

Panorama Management에서 클러스터 제거

Panorama 관리에서 클러스터를 제거하려면 **Panorama** > **Managed WildFire Clusters**를 선택한 다음 제거할 클러스터의 행을 선택한 다음(클러스터 이름을 클릭하지 않음) **Panorama**에서 제거를 선택합니다.

Panorama 관리에서 WildFire 어플라이언스 클러스터를 제거하면 Panorama 웹 인터페이스는 해당 클러스터의 WildFire 어플라이언스를 읽기 전용 모드로 전환합니다. 제거된 클러스터의 WildFire 어플라이언스가 Panorama 웹 인터페이스에 표시되지만 읽기 전용 모드에서는 구성을 WildFire 어플라이언스에 푸시하거나 Panorama로 관리할 수 없습니다. Panorama 관리에서 제거된 후 WildFire 어플라이언스 클러스터 구성원은 로컬 클러스터 구성을 사용하고 로컬 CLI를 사용하여 클러스터를 관리할 수 있습니다.

Panorama 관리에서 클러스터를 제거한 후 Panorama로 클러스터의 WildFire 어플라이언스를 관리하려면 클러스터를 Panorama로 다시 가져옵니다(**Panorama** > **Managed WildFire Clusters** > **Import Cluster Config**).

STEP 1 | 클러스터의 컨트롤러 노드를 선택합니다. 클러스터 이름은 클러스터를 자동으로 채웁니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 확인을 클릭합니다. 클러스터 백업 컨트롤러 노드와 작업자 노드가 자동으로 채워집니다.

STEP 3 | 확인을 클릭하여 클러스터를 가져옵니다.

STEP 4 | 변경 사항을 커밋합니다.

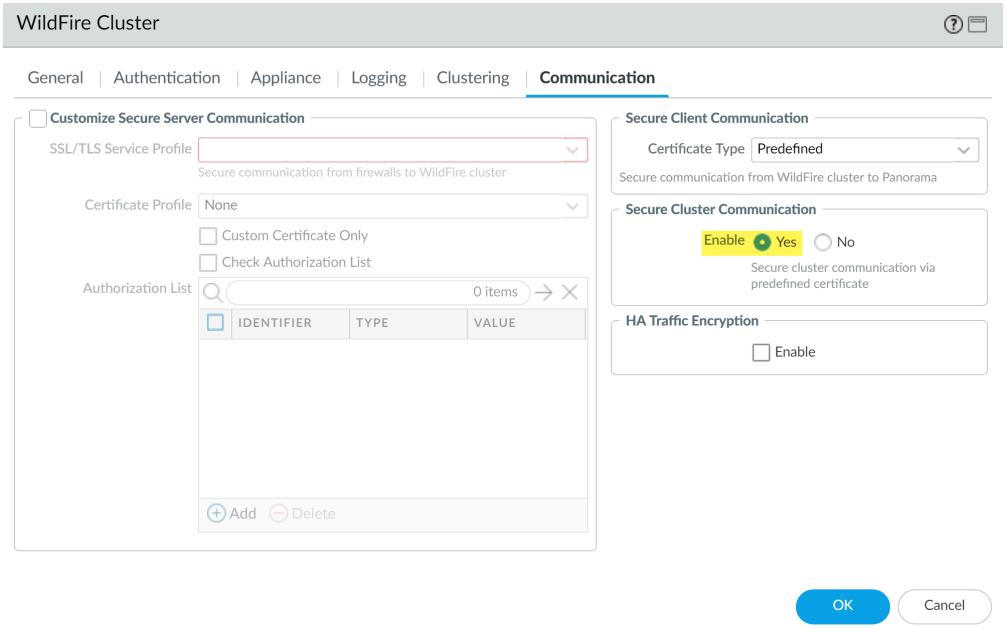
Panorama에서 중앙 집중식으로 사전 정의된 인증서를 사용하여 어플라이언스 간 암호화 구성

STEP 1 | 각 관리형 WildFire 어플라이언스를 PAN-OS 8.1.x로 업그레이드합니다. 모든 관리 대상 기기는 기기 간 암호화를 활성화하기 위해 PAN-OS 8.1 이상의 버전을 실행해야 합니다.

STEP 2 | WildFire 어플라이언스 클러스터가 올바르게 구성되었고 정상 상태에서 작동하는지 확인하십시오.

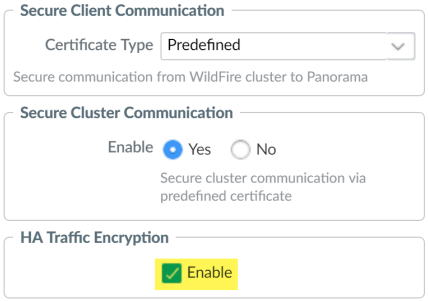
STEP 3 | Panorama에서 **Panorama >** 관리형 **WildFire** 클러스터 **> *WF_cluster_name>*** 통신을 선택합니다.

STEP 4 | 보안 클러스터 통신을 활성화합니다.



STEP 5 | (권장) HA 트래픽 암호화를 활성화합니다. 이 선택적 설정은 HA 쌍 간의 HA 트래픽을 암호화하며 Palo Alto Networks에서 권장하는 모범 사례입니다.

FIPS/CC 모드에서 작동하는 경우 *HA* 트래픽 암호화를 비활성화할 수 없습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 6 | 확인을 클릭하여 **WildFire** 클러스터 설정을 저장합니다.

STEP 7 | 변경 사항을 커밋합니다.

Panorama에서 중앙 집중식으로 사용자 지정 인증서를 사용하여 어플라이언스 간 암호화 구성

STEP 1 | 각 관리형 WildFire 어플라이언스를 PAN-OS 8.1.x로 업그레이드합니다. 모든 관리 대상 기기는 기기 간 암호화를 활성화하기 위해 PAN-OS 8.1 이상의 버전을 실행해야 합니다.

STEP 2 | WildFire 어플라이언스 클러스터가 올바르게 구성되었고 정상 상태에서 작동하는지 확인하십시오.

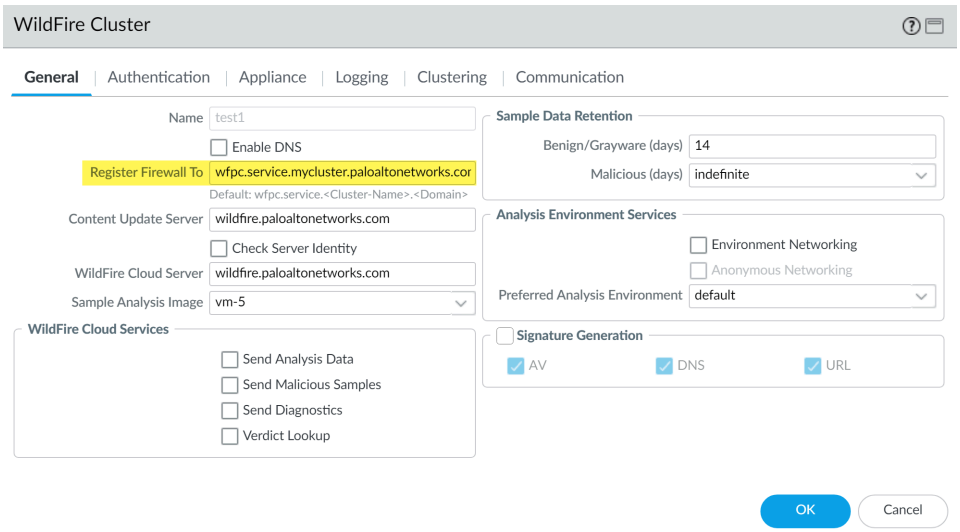
STEP 3 | 기존 WildFire 보안 통신 구성을 검토합니다. 이전에 사용자 지정 인증서를 사용하여 통신 보안을 위해 WildFire 어플라이언스와 방화벽을 구성한 경우 WildFire 어플라이언스 간의 통신 보안을 위해 해당 사용자 지정 인증서를 사용할 수도 있습니다.

1. **Panorama >**관리형 **WildFire** 클러스터**> *WF_cluster_name*>** 통신을 선택합니다.
2. 보안 서버 통신 사용자 지정이 활성화되어 있고 해당 인증서를 사용하려는 경우 사용 중인 사용자 지정 인증서의 세부 정보를 식별합니다. 그렇지 않으면 5단계로 진행하여 새 사용자 지정 인증서 설치 프로세스를 시작합니다.
3. 4단계에서 방화벽 등록 주소를 정의하는 데 사용할 사용자 지정 인증서 FQDN(DNS 이름)을 결정합니다.

> 사용자 지정 인증서 이름과 연결된 *FQDN*을 기록해 두십시오. 이는 구성 프로세스 중에 여러 번 참조됩니다.

STEP 4 | Panorama에서 방화벽 등록 주소를 구성합니다.

1. Panorama에서 **Panorama >**관리형 **WildFire** 클러스터**> *WF_cluster_name*>** 일반을 선택합니다.
2. 방화벽 등록 대상 필드에서 사용자 지정 인증서에 있는 인증에 사용되는 DNS 이름(일반적으로 SubjectName 또는 SubjectAltName)을 지정합니다. 예를 들어, 기본 도메인 이름은 **`wfpc.service.mycluster.paloaltonetworks.com`**입니다.



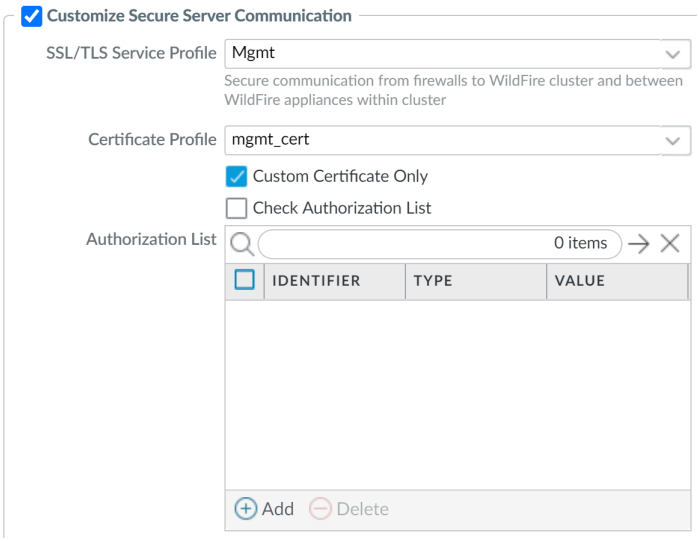
 ©2024 Palo Alto Networks, Inc.

STEP 5 | Panorama에서 WildFire 보안 서버 통신 설정을 구성합니다. 방화벽과 WildFire 클러스터 간의 통신 보안을 이미 구성했고 기존 사용자 지정 인증서를 사용 중인 경우 아래 4단계로 진행합니다.

1. Panorama에서 **Panorama>** 관리형 **WildFire** 클러스터**>** ***WF_cluster_name*>** 통신을 선택합니다.
2. 보안 서버 통신 사용자 지정을 클릭합니다.
3. WildFire 어플라이언스 및 관련 방화벽에 사용되는 사용자 지정 인증서를 구성하고 배포합니다. SSL/TLS 서비스 프로파일은 WildFire 어플라이언스 피어 및 방화벽과 통신하기 위해 WildFire 어플라이언스에서 사용하는 사용자 지정 인증서를 정의합니다. 또한 WildFire 어플라이언스 클러스터와 연결된 방화벽에서 사용자 지정 인증서 설정을 구성해야 합니다. 이것은 9단계의 뒷부분에서 구성됩니다.
   1. SSL/TLS 서비스 프로파일 드롭다운을 열고 SSL/TLS 서비스 프로파일을 클릭합니다. 사용하려는 사용자 지정 인증서로 SSL/TLS 서비스 프로파일을 구성합니다. SSL/TLS 서비스 프로파일을 구성한 후 확인을 클릭하고 새로 생성된 SSL/TLS 서비스 프로파일을 선택합니다.
   2. 인증서 프로파일 드롭다운을 열고 인증서 프로파일을 클릭합니다. 방화벽과 WildFire 어플라이언스 간, 그리고 피어 WildFire 어플라이언스 간에 보안 연결을 설정하는 데 사용되는 사용자 지정 인증서를 식별하는 인증서 프로파일을 구성합니다. 인증서 프로파일을 구성한 후 확인을 클릭하고 새로 생성된 프로파일을 선택합니다.
4. 사용자 지정 인증서만 확인란을 선택합니다. 이렇게 하면 기본 사전 구성된 인증서 대신 구성한 사용자 지정 인증서를 사용할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

5. (선택 사항) 권한 부여 목록을 구성합니다. 인증 목록은 사용자 지정 인증서 주체 또는 주체 대체 이름을 확인합니다. 사용자 지정 인증서와 함께 제공된 주체 또는 주체 대체 이름이 인증 목록의 식별자와 일치하지 않으면 인증이 거부됩니다.
   1. 권한 부여 목록을 추가합니다.
   2. 사용자 지정 인증서 프로파일에 구성된 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 식별자가 제목인 경우 일반 이름을 입력하고 식별자가 제목 대체 이름인 경우 IP 주소, 호스트 이름 또는 이메일을 입력합니다.
   4. 확인을 클릭합니다.
   5. 권한 부여 목록 확인을 선택하여 권한 부여 목록을 시행하십시오.
6. 확인을 클릭합니다.



STEP 6 | 보안 클러스터 통신을 활성화합니다.

STEP 7 | (권장) HA 트래픽 암호화를 활성화합니다. 이 선택적 설정은 HA 쌍 간의 HA 트래픽을 암호화하며 Palo Alto Networks에서 권장하는 모범 사례입니다.

FIPS/CC 모드에서 작동하는 경우 *HA* 트래픽 암호화를 비활성화할 수 없습니다.

STEP 8 | 확인을 클릭하여 **WildFire** 클러스터 설정을 저장합니다.

STEP 9 | WildFire 어플라이언스 클러스터를 방화벽 사용자 지정 인증서와 연결하도록 Panorama에서 방화벽 통신 보안 설정을 구성합니다. 이는 방화벽과 WildFire 어플라이언스 클러스터 간의 통신 보안 채널을 제공합니다. 방화벽과 WildFire 어플라이언스 클러스터 간에 통신 보안을 이미 구성했고 기존 사용자 지정 인증서를 사용 중인 경우 다음 단계로 진행합니다.

1. 디바이스 > 설정 > 관리 > 통신 보안 설정을 선택하고 통신 보안 설정에서 편집 아이콘을 클릭하여 방화벽 사용자 지정 인증서 설정을 구성합니다.
2. 각 드롭다운에서 인증서 유형, 인증서 및 인증서 프로파일을 선택하고 사용자 지정 인증서를 사용하도록 구성합니다.

 ©2024 Palo Alto Networks, Inc.

3. 통신 사용자 정의에서 **WildFire** 통신을 선택하십시오.
4. 확인을 클릭합니다.

STEP 10 | 변경 사항을 커밋합니다.

Panorama를 사용하여 WildFire 클러스터 상태 보기

구성된 WildFire 어플라이언스 클러스터가 올바르게 작동하는지 확인하기 위해 Panorama 어플라이언스를 사용하여 현재 상태를 볼 수 있습니다.

*Palo Alto Networks*는 *WildFire* 어플라이언스 *CLI*를 사용하여 *WildFire* 클러스터의 상태를 확인할 것을 권장합니다. *Panorama*에서 볼 수 없는 추가 상태 세부 정보는 명령 출력에 표시됩니다.

STEP 1 | 기본 Panorama 어플라이언스에서 **Panorama >** 관리형 **WildFire** 클러스터를 선택합니다.

STEP 2 | 클러스터 상태 열에서 다음을 확인합니다.

1. wfpc 및 서명 서비스가 실행 중입니다.
2. 다른 작업이 없습니다. 비정상 작동 및 해당 상태 조건은 다음과 같습니다.
   - 폐기 [요청됨/진행 중/거부됨/성공/실패]
   - 일시 중단 [요청됨/진행 중/거부됨/성공/실패]
   - 재부팅 [요청됨/진행 중/거부됨/성공/실패]
   - 클러스터 [오프라인 / splitbrain / 준비되지 않음]
   - 서비스 [중단/없음]
   - HA [peer-offline / cfg-not-sync / cfg-sync-off]

STEP 3 | 구성 상태 열에서 다음을 확인합니다.

1. 어플라이언스 구성은 Panorama 어플라이언스에 저장된 구성과 동기화됩니다.
2. 다른 상태가 없습니다. 비정상적인 상태 조건은 다음과 같습니다.
   - 동기화되지 않음 [어플라이언스 구성이 Panorama에 저장된 구성과 동기화되지 않았습니다. 돋보기 위로 마우스를 가져가면 동기화 실패의 원인을 표시할 수 있습니다].

STEP 4 | 연결됨 열에서 구성된 WildFire 어플라이언스가 연결됨 상태를 표시하는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

 ©2024 Palo Alto Networks, Inc.

라이선스 및 업데이트 관리

Panorama™ 관리 서버를 사용하여 방화벽 및 전용 로그 수집기에서 라이선스, 소프트웨어 업데이트 및 콘텐츠 업데이트를 중앙에서 관리할 수 있습니다. 라이선스 또는 업데이트를 배포할 때 Panorama는 Palo Alto Networks® 라이선스 서버 또는 업데이트 서버에 체크인하고 요청 유효성을 확인한 다음 라이선스 또는 업데이트의 검색 및 설치를 허용합니다. 이 기능은 각 방화벽 또는 전용 로그 수집기에서 동일한 작업을 반복할 필요가 없도록 하여 배포를 용이하게 합니다. 인터넷에 직접 액세스할 수 없는 방화벽을 관리하거나 웹 인터페이스가 없는 전용 로그 수집기를 관리하는 데 특히 유용합니다.

업데이트를 배포하기 전에 업데이트 버전 호환성에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.

각 방화벽에서 직접 지원 구독을 활성화해야 합니다. Panorama를 사용하여 지원 구독을 배포할 수 없습니다.

Panorama 관리 서버에서 라이선스를 활성화하거나 업데이트를 설치하려면 Panorama 등록 및 라이선스 설치 및 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치를 참조하십시오.

- Panorama를 사용하여 방화벽에서 라이선스 관리

Panorama를 사용하여 방화벽에서 라이선스 관리

다음 단계에서는 인증(인증) 코드를 사용하여 새 라이선스를 검색하고 라이선스 키를 관리되는 방화벽에 푸시하는 방법을 설명합니다. 또한 직접 인터넷 액세스가 가능한 방화벽과 직접 인터넷 액세스가 없는 방화벽의 라이선스 상태를 수동으로 업데이트(새로 고침) 하는 방법에 대해서도 설명합니다. Panorama™는 자동으로 라이선스 서버에 일일 체크인을 수행하고 라이선스 업데이트 및 갱신을 검색하여 방화벽으로 푸시합니다. 체크인은 오전 1시에서 오전 2시 사이에 발생하도록 하드 코딩되어 있습니다. 이 일정을 변경할 수 없습니다.

*Panorama*를 사용하여 방화벽에 대한 지원 라이선스를 활성화할 수 없습니다. 지원 라이선스를 활성화하려면 방화벽에 개별적으로 액세스해야 합니다.

Panorama 라이선스를 활성화하려면 Panorama 등록 및 라이선스 설치를 참조하십시오.

- 새로 구입한 라이선스를 활성화합니다.
  1. **Panorama** > 디바이스 배포 > 라이선스를 선택한 다음 활성화합니다.
  2. 새 라이선스가 있는 각 방화벽에 대해 Palo Alto Networks®에서 제공한 인증 코드를 입력합니다.
  3. 라이선스를 활성화합니다.
  4. (WildFire® 구독만 해당) 새 WildFire 구독이 있는 각 방화벽에서 커밋을 수행하여 활성화를 완료합니다.
     - 보류 중인 변경 사항을 커밋합니다. 이를 수행하려면 각 방화벽 웹 인터페이스에 액세스해야 합니다.
     - 보류 중인 구성 변경 사항이 없으면 약간 변경하고 커밋합니다. 예를 들어 규칙 설명을 업데이트하고 변경 사항을 커밋합니다. 방화벽이 동일한 디바이스 그룹에 속하는 경우 Panorama에서 규칙 변경을 푸시하여 각 방화벽에 개별적으로 액세스하는 대신 모든 방화벽에서 커밋을 시작할 수 있습니다.

     WildFire 분석 프로파일 규칙에 *WildFire* 구독이 지원하는 *Advanced* 파일 유형이 포함되어 있는지 확인하십시오.

- 방화벽의 라이선스 상태를 업데이트합니다.
  1. **Panorama** > 디바이스 배포 > 라이선스를 선택합니다.

     페이지의 각 항목은 라이선스가 활성 또는 비활성인지의 여부를 나타내며 활성 라이선스의 만료 날짜를 표시합니다.
  2. 이전에 방화벽에서 직접 지원 구독에 대한 인증 코드를 활성화한 경우 새로 고침을 클릭하고 목록에서 방화벽을 선택합니다. Panorama는 라이선스를 검색하여 방화벽에 배포하고 Panorama 웹 인터페이스에서 라이선스 상태를 업데이트합니다.
  3. (Enterprise Data Loss Prevention(DLP) 라이선스만 해당) Enterprise DLP를 활용하는 관리형 방화벽에 업데이트된 라이선스를 푸시합니다.
     1. 커밋 및 **Panorama**에 커밋을 선택합니다.
     2. 커밋 > 디바이스에 푸시를 선택한 다음 선택 사항을 편집합니다.

©2024 Palo Alto Networks, Inc.

3. 템플릿을 선택한 다음 Enterprise DLP를 활용하는 관리형 방화벽과 연결된 템플릿 스택(template stack)을 선택합니다.

   계속하려면 확인을 클릭하세요.
4. 템플릿 구성을 푸시하여 Enterprise DLP 라이선스를 성공적으로 업데이트합니다.

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

네트워크 활동 모니터링

Panorama™ 관리 서버는 네트워크 트래픽에 대한 종합적인 그래픽 보기를 제공합니다. Panorama의 가시성 도구인 ACC(Application Command Center), 로그 및 보고서 생성 기능을 사용하여 모든 네트워크 활동을 중앙에서 분석, 조사 및 보고하고 잠재적인 보안 영향이 있는 영역을 식별하고 이를 안전한 애플리케이션 활성화 정책으로 변환할 수 있습니다. .

이 섹션에서는 다음 항목을 다룹니다.

- 가시성을 위해 Panorama 사용
- Panorama의 ESM 로그 수집 트랩
- 사용 사례: Panorama를 사용하여 애플리케이션 모니터링
- 사용 사례: Panorama를 사용하여 사고에 대응

가시성을 위해 Panorama 사용

Panorama는 중앙 배포 및 방화벽 구성 기능 외에도 네트워크를 통과하는 모든 트래픽을 모니터링하고 보고할 수 있습니다. Panorama와 방화벽의 보고 기능은 매우 유사하지만 Panorama가 제공하는 이점은 관리되는 모든 방화벽에서 집계된 정보를 단일 창에서 볼 수 있다는 것입니다. 이 집계된 보기는 전체 네트워크에서 사용자 활동, 트래픽 패턴 및 잠재적 위협의 추세에 대한 실행 가능한 정보를 제공합니다.

ACC(Application Command Center), App-Scope, 로그 뷰어 및 Panorama의 사용자 지정 가능한 표준 보고 옵션을 사용하여 네트워크를 통과하는 트래픽에 대해 빠르게 알아볼 수 있습니다. 이 정보를 볼 수 있는 기능을 통해 현재 정책이 적절한 부분과 불충분한 부분을 평가할 수 있습니다. 그런 다음 이 데이터를 사용하여 네트워크 보안 전략을 강화할 수 있습니다. 예를 들어 보안 규칙을 강화하여 네트워크의 모든 사용자에 대한 규정 준수 및 책임을 높이거나 네트워크 용량을 관리하고 자산에 대한 위험을 최소화하면서 네트워크 사용자의 다양한 애플리케이션 요구 사항을 충족할 수 있습니다.

다음 주제는 자체 네트워크 인프라 내에서 이러한 기능을 사용하는 방법을 설명하는 몇 가지 사용 사례를 포함하여 Panorama의 보고 기능에 대한 높은 수준의 보기를 제공합니다. 사용 가능한 보고서 및 차트의 전체 목록과 각각에 대한 설명은 온라인 도움말을 참조하십시오.

- ACC 및 AppScope로 네트워크 모니터링
- 로그 데이터 분석
- 보고서 생성, 예약 및 이메일로 보내기
- 예약된 보고서에 대한 주요 제한 구성

ACC 및 AppScope로 네트워크 모니터링

ACC와 AppScope를 사용하면 네트워크를 통과하는 트래픽에서 기록된 데이터를 모니터링하고 보고할 수 있습니다.

Panorama의 ACC는 네트워크 트래픽 요약을 표시합니다. Panorama는 네트워크의 모든 관리 방화벽에서 데이터를 동적으로 쿼리하여 ACC에 표시할 수 있습니다. 이 디스플레이를 통해 Palo Alto Networks 차세대 방화벽의 전체 네트워크에서 애플리케이션, 사용자 및 콘텐츠 활동(URL 카테고리, 위협, 데이터 또는 파일을 효과적으로 차단하는 보안 정책)별로 트래픽을 모니터링할 수 있습니다.

AppScope는 네트워크에서 예상치 못한 또는 비정상적인 동작을 한 눈에 식별하는 데 도움이 됩니다. 여기에는 위협 또는 애플리케이션별로 또는 플로우의 소스 또는 대상별로 트래픽 플로우을 분석할 수 있는 요약 보고서, 변경 모니터, 위협 모니터, 위협 맵, 네트워크 모니터, 트래픽 맵과 같은 일련의 차트 및 보고서가 포함됩니다. 세션 또는 바이트 수를 기준으로 정렬할 수도 있습니다.



디바이스 그룹 및 템플릿 관리자는 액세스 도메인 내의 디바이스 그룹에 대한 네트워크 및 ACC 데이터만 할 수 있습니다.

ACC 및 AppScope를 사용하여 다음과 같은 질문에 답하십시오.

 ©2024 Palo Alto Networks, Inc.

ACC	모니터 > 앱스코프
• 네트워크에서 가장 많이 사용되는 애플리케이션은 무엇이며 고위험 애플리케이션은 몇 개입니까? 네트워크에서 고위험 애플리케이션의 상위 사용자는 누구입니까? • 지난 1시간 동안 조회된 상위 URL 카테고리는 무엇입니까?	• 애플리케이션 사용 트렌드는 무엇입니까? 사용이 증가한 상위 5개 애플리케이션과 사용이 감소한 상위 5개 애플리케이션은 무엇입니까? • 지난 주 또는 지난 달과 비교하여 이번 주 동안 사용자 활동이 어떻게 변경되었습니까?
• 대역폭을 가장 많이 사용하는 애플리케이션은 무엇입니까? 가장 높은 대역폭을 사용하는 사용자/호스트는 누구입니까? • 어떤 콘텐츠 또는 파일이 차단되고 있으며 이 파일 차단/데이터 필터링 규칙을 트리거하는 특정 사용자가 있습니까? • 두 개의 특정 IP 주소 간에 교환되거나 특정 사용자가 생성한 트래픽의 양은 얼마입니까? 대상 서버 또는 클라이언트는 지리적으로 어디에 있습니까?	• 어떤 사용자와 애플리케이션이 네트워크 대역폭의 대부분을 차지합니까? 그리고 이 소비는 지난 30일 동안 어떻게 바뀌었습니까? • 네트워크의 위협은 무엇이며 이러한 들어오고 나가는 트래픽 위협은 지리적으로 어떻게 분산되어 있습니까?

그런 다음 정보를 사용하여 네트워크의 트래픽 패턴을 유지 관리하거나 변경 사항을 적용할 수 있습니다. Panorama의 가시성 도구가 네트워크에 대한 허용 가능한 사용 정책을 형성하는 방법에 어떻게 영향을 미칠 수 있는지에 대해서는 사용 사례: Panorama를 사용하여 애플리케이션 모니터링을(를) 참조하십시오.

다음은 ACC 탐색에 도움이 되는 몇 가지 팁입니다.

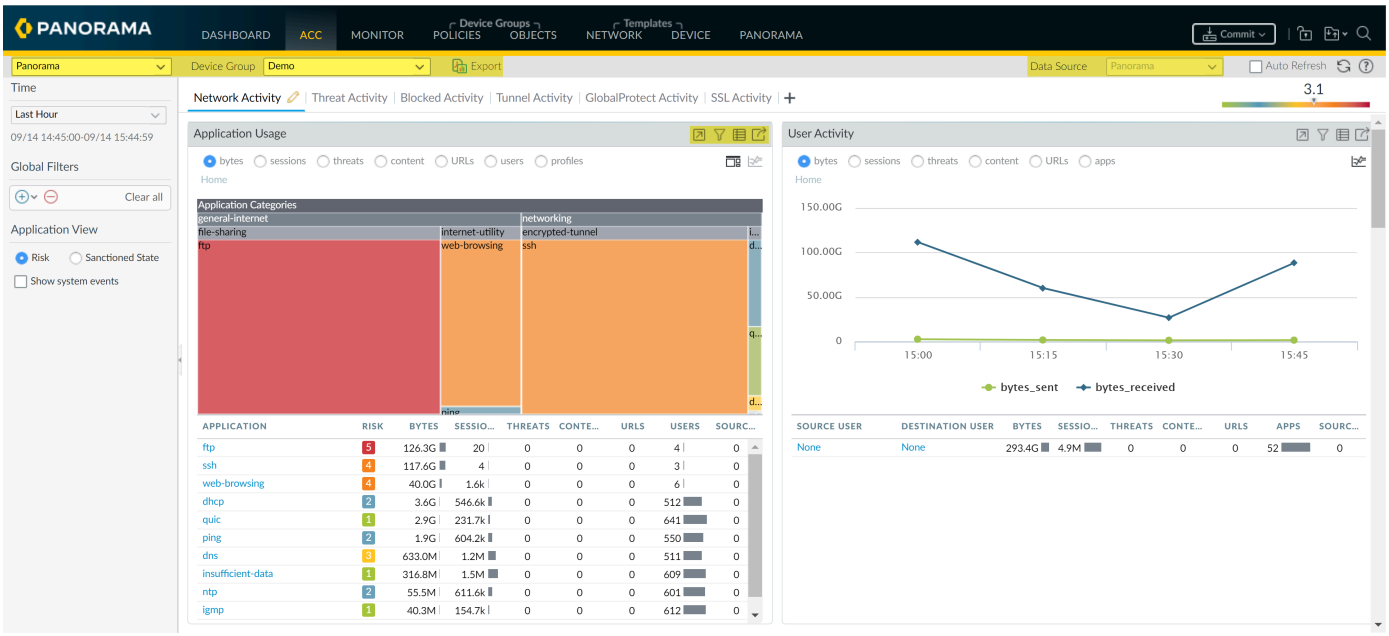


그림 **24: ACC** 탐색 팁

©2024 Palo Alto Networks, Inc.

- **Panorama** 보기에서 디바이스 보기로 전환 - 컨텍스트 드롭다운을 사용하여 관리되는 방화벽의 웹 인터페이스에 액세스합니다. 자세한 내용은 컨텍스트 스위치 - 방화벽 또는 Panorama을(를) 참조하십시오.
- 디바이스 그룹 및 데이터 소스 변경 - ACC의 차트에 통계를 표시하는 데 사용되는 기본 데이터 소스는 **Panorama** 로컬 데이터이고 기본 디바이스 그룹 설정은 모두입니다. Panorama에서 로컬 데이터를 사용하면 차트를 빠르게 로드할 수 있습니다. 그러나 모든 관리 방화벽이 PAN-OS 7.0 이상 버전에 있는 경우 데이터 소스를 원격 디바이스 데이터로 변경할 수 있습니다. 관리 방화벽에 PAN-OS 7.0 및 이전 버전이 혼합되어 있는 경우 Panorama 데이터만 볼 수 있습니다. 원격 디바이스 데이터를 사용하도록 구성된 경우 Panorama는 관리되는 모든 방화벽을 폴링하고 데이터의 집계 보기를 표시합니다. 온스크린(onscreen) 디스플레이는 폴링되는 총 방화벽 수와 정보 쿼리에 응답한 방화벽 수를 나타냅니다.
- 볼 탭 및 위젯 선택 - ACC에는 관심 있는 정보를 찾을 수 있도록 하는 세 개의 탭과 위젯 배열이 포함되어 있습니다. 애플리케이션 사용 위젯 및 호스트 정보 위젯을 제외하고 다른 모든 위젯은 해당 기능이 방화벽에서 라이선스되고 로깅을 활성화한 경우에만 데이터를 표시합니다.
- 시간 프레임 조정 및 데이터 수정 - ACC의 보고 기간은 지난 15분에서 마지막 시간, 일, 주, 월 또는 사용자 정의 시간 범위입니다. 기본적으로 각 위젯은 상위 10개 항목을 표시하고 나머지 모든 항목을 다른 항목으로 집계합니다. 세션, 바이트, 위협, 콘텐츠 및 URL과 같은 다양한 속성을 사용하여 각 위젯의 데이터를 정렬할 수 있습니다. 또한 로컬 필터를 설정하여 위젯의 테이블 및 그래프 내 표시를 필터링한 다음 위젯 필터를 전역 필터로 승격하여 ACC의 모든 위젯에서 보기를 피벗할 수 있습니다.

로그 데이터 분석

Panorama의 모니터 탭은 로그 데이터에 대한 액세스를 제공합니다. 이러한 로그는 관리되는 방화벽에서 처리되고 Panorama로 전달된 아카이브된 세션 목록입니다.

로그 데이터는 애플리케이션, 위협, 호스트 정보 프로필, URL 범주, 콘텐츠/파일 유형과 같은 네트워크의 트래픽 흐름에 대한 세부 정보와 시스템 이벤트, 구성 변경 및 사용자- ID™ 매핑 정보.

관리되는 방화벽의 로그 포워딩 구성에 따라 **Monitor** > **Logs** 탭에는 트래픽 흐름, 위협, URL 필터링, 데이터 필터링, 호스트 정보 프로필(HIP) 일치 및 WildFire™ 제출에 대한 로그가 포함될 수 있습니다. 로그를 검토하여 주어진 세션 또는 트랜잭션에 대한 풍부한 정보를 확인할 수 있습니다. 이 정보의 몇 가지 예는 세션을 시작한 사용자, 방화벽이 세션에서 수행한 작업(허용 또는 거부), 소스 및 대상 포트, 영역 및 주소입니다. 시스템 및 구성 로그는 구성된 임계값이 초과되었을 때 방화벽이 트리거한 구성 변경 또는 경보를 나타낼 수 있습니다.

*Panorama*가 *PAN-OS 7.0* 이전 버전의 소프트웨어를 실행하는 방화벽을 관리할 경우 *Panorama*가 해당 방화벽이 제출하는 *WildFire* 샘플에 대한 분석 정보를 수집할 수 있는 *WildFire* 서버를 지정하십시오. *Panorama*는 이 정보를 사용하여 *PAN-OS 7.0*에 도입된 필드 값이 누락된 *WildFire* 제출 로그를 완성합니다. 이전 릴리스를 실행하는 방화벽은 해당 필드를 채우지 않습니다. 서버를 지정하려면 ***Panorama*** > ***Setup*** > ***WildFire***를 선택하고 일반 설정을 편집한 다음 ***WildFire Private Cloud*** 이름을 입력합니다. 기본값은 미국에서 호스팅되는 *WildFire* 클라우드인 ***wildfire-public-cloud***,입니다.

보고서 생성, 예약 및 이메일로 보내기

보고서가 즉시 실행되도록 구성하거나 특정 간격으로 실행되도록 예약할 수 있습니다. 보고서를 저장하고 내보내거나 특정 수신자에게 이메일로 보낼 수 있습니다. 이메일은 Panorama에 대한 액세스 권한이 없는

 ©2024 Palo Alto Networks, Inc.

관리자와 보고서를 공유하려는 경우에 특히 유용합니다. Panorama는 Palo Alto Networks 방화벽과 동일한 보고서 유형을 지원합니다.

Panorama 10.0.2 및 Cloud Services 플러그인 버전 1.8.0부터 Strata Logging Service 데이터에 대한 예약 보고서를 생성할 수 있습니다. 이 설정은 기본적으로 비활성화되어 있으며 Panorama에서 수동으로 활성화해야 합니다. 이 설정 상태(활성화 또는 비활성화)는 PAN-OS 업그레이드, 다운그레이드 및 Cloud Services 플러그인 제거 시 지속됩니다. Strata Logging Service 데이터에서 보고서를 생성하려면 먼저 Panorama CLI에서 기능을 활성화해야 합니다.

보고서를 생성할 방화벽 및 *Panorama*에 일치하는 소프트웨어 버전을 설치하는 것이 좋습니다. 예를 들어, *Panorama* 관리 서버가 *Panorama 10.0*을 실행하는 경우 보고서를 생성하기 전에 관리형 방화벽에 *PAN-OS 11.1*을 설치하십시오. 이 방법은 *Panorama* 버전에서 지원되지만 방화벽의 이전 *PAN-OS* 버전에서는 지원되지 않는 필드를 포함하는 보고서를 생성하는 경우 발생할 수 있는 문제를 방지합니다.

STEP 1 | (Strata Logging Service 전용) Panorama에서 예약 보고서를 활성화합니다.

1. Panorama CLI에 로그인.
2. 예약된 보고서 설정을 활성화합니다.

```
admin> request plugins cloud_services logging-service sched-report-enable
```

3. 구성 변경을 커밋합니다.

```
admin>  configure
```

```
admin#  commit force
```

4. 예약된 보고서 설정이 활성화되어 있는지 확인합니다.

```
admin> show system state | match sched-report
```

출력은 `cfg.report.lcass-sched-reports-enabled: True`로 활성화된 경우에 표시됩니다.

출력은 `cfg.report.lcass-sched-reports-enabled: False`으로 비활성화된 경우 표시되거나 출력이 반환되지 않습니다.

©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama 사전 정의 보고서를 구성합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고를 편집합니다.
2. 로그 내보내기 및 보고를 선택한 다음 사전 정의된 보고서에 데이터 사용 을 활성화(선택)하여 시간별 보고서 집계를 로그 수집기로 오프로드합니다.

   (Strata Logging Service 전용) 이 단계는 Strata Logging Service에 저장된 로그의 예약 보고서를 생성하는 데 필요합니다.

   > *VM-50*, *VM-50 Lite* 및 *PA-200* 방화벽에 대해 이 설정을 활성화하는 것이 좋습니다. 다른 모든 관리형 방화벽 모델에서는 이 설정을 활성화하는 것이 선택 사항입니다.

3. 사전 정의된 보고서를 선택한 다음 사전 정의된 보고서를 활성화(확인)하여 Panorama에서 푸시합니다.
4. 커밋 > **Panorama**에 커밋을 선택한 다음 구성 변경 사항을 커밋합니다.
5. (VM-50, VM-50 Lite 및 PA-200 방화벽만 해당) 방화벽 CLI에 액세스하여 사전 정의된 보고서를 활성화합니다.

   이 명령은 각 VM-50, VM-50 Lite 및 PA-200 방화벽에서 실행해야 합니다.

   ```
   admin> debug run-panorama-predefined-report yes
   ```

STEP 3 | 방화벽에서 수신하는 사용자 및 사용자 그룹 정보를 수신하고 저장하도록 Panorama를 구성합니다.

IP 주소 대신 사용자 이름과 그룹을 기반으로 보고서를 생성하는 데 필요합니다.

1. Panorama가 보고서에 사용자 그룹 정보를 포함하도록 하려면 관리 방화벽을 PAN-OS 8.1 이상 버전으로 업그레이드하십시오. Panorama는 이전 릴리스를 실행하는 방화벽의 그룹 정보를 동기화할 수 없습니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 Panorama 설정을 편집하고 그룹에 대한 보고 및 필터링 활성화를 선택합니다.
3. 아직 하지 않은 경우 디바이스 그룹을 추가하십시오. 각 디바이스 그룹에 대해:
   - Panorama에 사용자 및 사용자 그룹 정보를 제공하는 방화벽인 마스터 디바이스를 선택합니다.
   - Panorama를 활성화하여 마스터 디바이스에서 사용자 및 그룹을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 4 | 보고서를 생성합니다.

동일한 데이터베이스 및 기간에 대한 예약 및 지금 실행 요약 보고서는 각 보고서에 표시되는 데이터에 차이가 있습니다. 이는 로그 수집기 및 방화벽이 시간별 집계 중에 로그를 집계하는 방식 때문입니다.

보고서 생성 단계는 유형에 따라 다릅니다.

- 맞춤 보고서:
  1. 모니터 > 맞춤형 보고서 관리를 선택하고 보고서를 추가합니다.
  2. 보고서를 식별할 이름을 입력합니다.
  3. 보고서에 대한 데이터베이스를 선택합니다.

     요약 데이터베이스 또는 세부 로그 데이터베이스를 기반으로 보고서를 작성할 수 있습니다.

     Panorama 관리 서버 및 로그 수집기에 저장된 로그를 기반으로 보고서를 작성하려면 **Panorama Data**(빠른 성능을 위해 권장됨)를 선택합니다.

     관리되는 방화벽에 저장된 로그를 기반으로 보고서를 작성하려면 원격 디바이스 데이터를 선택하십시오. 이 옵션은 방화벽에 Panorama로 아직 포워딩되지 않은 로그가 있을 수 있는 경우에 사용합니다. 그러나 Panorama는 방화벽을 직접 쿼리해야 하므로 이 옵션은 더 느립니다.
  4. 예약됨을 선택합니다.
  5. 보고서에 표시할 시간 프레임, 정렬 기준 순서, 그룹화 기준 기본 설정 및 열(로그 속성)을 선택하여 로그 필터링 기준을 정의합니다.

     정확한 보고서를 생성하려면 정렬 기준 순서를 선택해야 합니다. 정렬 기준 순서를 선택하지 않으면 생성된 사용자 정의 보고서가 선택한 데이터베이스에 대해 가장 최근에 일치하는 로그로 채워집니다.
  6. 사용 가능한 열 목록에서 보고서에 표시할 열을 선택하고 선택한 열 목록에 추가합니다.

     추가한 열은 선택한 열 목록에 나타납니다. 보고서를 저장하거나 실행하려면 하나 이상의 열을 추가해야 합니다.

     예약된 보고서를 생성하려면 정렬별 목록에서 선택한 필드를 선택한 열 목록에 추가해야 합니다.
  7. (선택 사항) 쿼리 빌더를 사용하여 로그 속성을 기반으로 로그 필터링 기준을 더욱 세분화합니다.
  8. 보고서 설정을 테스트하려면 지금 실행을 선택합니다. 필요한 경우 설정을 수정하여 보고서에 표시되는 정보를 변경합니다.
  9. 확인을 클릭하여 사용자 정의 보고서를 저장합니다.
- **PDF** 요약 보고서:
  1. **PDF** 보고서 > 모니터링 > **PDF** 요약 관리를 선택한 다음 보고서를 추가합니다.
  2. 보고서를 식별할 이름을 입력합니다.
  3. 각 보고서 그룹에 대한 드롭다운을 사용하고 PDF 요약 보고서를 디자인할 요소를 하나 이상 선택합니다. 최대 18개의 요소를 포함할 수 있습니다.
  4. 확인을 클릭하여 설정을 저장합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 보고서 그룹을 구성합니다.

여기에는 사전 정의된 보고서, PDF 요약 보고서 및 사용자 정의 보고서가 포함될 수 있습니다. Panorama는 포함된 모든 보고서를 단일 PDF로 컴파일합니다.

1. 모니터 > **PDF** 보고서 > 보고서 그룹을 선택하고 보고서 그룹을 추가합니다.
2. 보고서 그룹을 식별할 이름을 입력합니다.
3. (선택사항) 제목 페이지를 선택한 다음 PDF 출력에 대한 제목을 추가합니다.
4. 사전 정의된 보고서, 사용자 정의 보고서 및 PDF 요약 보고서 목록에서 보고서를 선택합니다.
5. 선택한 보고서를 보고서 그룹에 추가합니다.
6. 확인을 클릭하여 설정을 저장합니다.

STEP 6 | 이메일 서버 프로파일을 구성합니다.

프로파일은 방화벽이 서버에 연결하고 이메일을 보내는 방법을 정의합니다.

1. **Panorama** > 서버 프로파일 > 이메일을 선택한 다음 서버 프로파일을 추가합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 최대 4개의 SMTP 서버를 추가하고 각각에 대해 다음 정보를 추가합니다.
   - 이름 - SMTP 서버를 식별하기 위한 이름입니다(1~31자). 이 필드는 레이블일 뿐이며 기존 서버의 호스트 이름일 필요는 없습니다.
   - 이메일 표시 이름 - 이메일의 보낸 사람 필드에 표시할 이름입니다.
   - 보낸 사람 - 알림 이메일을 보낼 이메일 주소입니다.
   - 받는 사람 - 알림 이메일이 전송될 이메일 주소입니다.
   - 추가 수신자 - 두 번째 계정으로 알림을 보내려면 여기에 추가 주소를 입력하십시오.
   - 이메일 게이트웨이 - 이메일을 보내는 데 사용할 SMTP 게이트웨이의 IP 주소 또는 호스트 이름입니다.
4. 확인을 클릭하여 프로파일을 저장합니다.

STEP 7 | 이메일 배달 보고서를 예약합니다.

1. 모니터 > **PDF** 보고서 > 이메일 스케줄러 및 이메일 스케줄러 프로파일 추가를 선택합니다.
2. 프로파일을 식별하려면 이름을 입력합니다.
3. 보고서 그룹, 방금 생성한 이메일 서버 프로파일(이메일 프로파일) 및 보고서에서 반복(기본값은 비활성화)을 선택합니다.
4. 테스트 이메일을 보내 이메일 설정이 정확한지 확인하십시오.
5. 확인을 클릭하여 변경 사항을 저장합니다.
6. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

예약된 보고서에 대한 주요 제한 구성

Panorama™ 관리 서버 및 PA-7000 시리즈 방화벽 보고서는 하나 이상의 Log Collector에서 키(집계할 수 있는 고유 값)를 활용하여 보고서를 작성하고 생성합니다. 예약된 보고서의 정확성을 개선하기 위해 이

 ©2024 Palo Alto Networks, Inc.

제 최대 및 최소 키 제한을 구성할 수 있습니다. 지원되는 키의 수를 늘려 예약된 보고서에 집계, 정렬 및 그룹화할 수 있는 더 많은 데이터를 포함할 수 있습니다.

기본 최소 키 제한은 다음 계산을 사용하여 예약된 보고서에 대해 구성된 정렬 기준 및 그룹화 기준 값을 기반으로 합니다.

<Sort By value> x 100 x <Group By value>

예를 들어 정렬 기준이 상위 **25**개로 구성되고 그룹 기준이 **5**개의 그룹으로 구성된 경우 기본 최소 키 제한은 12,500개의 키입니다. 없음으로 설정된 경우 그룹화 기준 값은 계산에 포함되지 않습니다. 기본 최소 키 제한은 최대 키 제한으로 제한되며 이를 초과할 수 없습니다.

M-시리즈 어플라이언스 및 *Panorama* 가상 어플라이언스에 대한 키 제한만 구성할 수 있습니다. *PA-7000* 시리즈 키 제한은 구성할 수 없습니다.

다음 Panorama 모델에 대해 지원되는 최대 및 최소 키가 증가합니다.

Panorama 모델	최소 키 제한	최대 키 제한
PA-7000 시리즈	1,000 - 기본값, 구성 불가	25,000 - 기본값, 구성 불가
M-200	15,000	50,000
M-500	15,000	50,000
M-600	15,000	50,000
레거시 모드의 Panorama 가상 어플라이언스	5,000	25,000
Panorama 가상 어플라이언스(지원되는 모든 모델)	15,000	50,000

STEP 1 | Panorama CLI에 로그인합니다.

STEP 2 | 다음 명령을 사용하여 최대 키 제한을 구성합니다.

최대 키 제한은 0과 50 사이에서 설정할 수 있습니다. 여기서 50은 50,000개의 키와 같습니다. 이 예에서는 Panorama 가상 어플라이언스의 최대 키 제한을 30,000개의 키로 설정합니다.

```
admin@Panorama> request max-report-keys set limit <Key Limit>
```

```
admin@Panorama> request max-report-keys set limit 30

cfg.report.max-keys-limit: 30
```


©2024 Palo Alto Networks, Inc.

STEP 3 | 다음 명령을 사용하여 최소 키 제한을 구성합니다.

최소 키 제한은 0에서 15 사이로 설정할 수 있습니다. 여기서 15는 15,000개의 키와 같습니다. 이 예에서는 Panorama 가상 어플라이언스에 대한 최소 키 제한을 15,000개의 키로 설정합니다.

```
admin@Panorama> request min-report-keys set limit <Key Limit>
```

```
admin@Panorama> request min-report-keys set limit 15

cfg.report.min-keys-limit: 15
```

STEP 4 | (선택 사항) 최소 키 제한을 기본 설정으로 설정합니다.

```
admin@Panorama> request min-report-keys set limit 0
```

STEP 5 | 다음 명령을 사용하여 Panorama에 새로운 최대 및 최소 키 제한을 커밋합니다.

```
admin@Panorama> commit-all
```

 ©2024 Palo Alto Networks, Inc.

Panorama의 ESM 로그 수집 트랩

가시성은 공격의 영향을 예방하고 줄이는 중요한 첫 번째 단계입니다. 이 문제를 해결하는 데 도움이 되도록 Panorama는 의심스럽거나 악의적인 활동을 추적할 수 있도록 방화벽 로그(네트워크의 이벤트) 및 Traps™ ESM Server 로그(엔드포인트의 보안 이벤트)에 대한 통합 보기를 제공합니다.

네트워크 및 엔드포인트에서 관찰된 이벤트에 대한 인식 및 컨텍스트를 위해 Traps 에이전트가 ESM Server에 보고하는 보안 이벤트를 Panorama에 포워딩합니다. Panorama는 TCP, UDP 또는 SSL을 통해 Syslog를 사용하여 Traps ESM 구성 요소에서 이러한 로그를 수집하는 Syslog 수신기 역할을 할 수 있습니다. 그런 다음 Panorama는 엔드포인트에서 발생하는 개별 보안 이벤트를 네트워크에서 발생하는 것과 연관시키고 일치 증거를 생성할 수 있습니다. 이 증거는 문제를 조사하고 네트워크의 보안 허점을 수정하기 위해 이벤트의 시간과 흐름에 대한 더 많은 컨텍스트를 제공합니다.

STEP 1 | Panorama에서 로그 수집 프로파일을 정의하고 수집기 그룹에 연결합니다.

레거시 모드의 *Panorama* 가상 어플라이언스는 트랩 로그를 수집할 수 없습니다.

1. **Panorama** > 로그 수집 프로파일을 선택한 다음 추가를 클릭합니다.
2. 프로필의 이름을 입력합니다.
3. 추가를 클릭하고 ESM 서버에 대한 세부 정보를 입력합니다. 프로파일에 최대 4개의 ESM 서버를 추가할 수 있습니다.
   1. 소스 이름을 입력합니다.
   2. Panorama가 syslog 메시지를 수신할 포트를 지정합니다. 범위는 23000~23999입니다.
   3. 전송 계층 프로토콜(TCP, UDP 또는 SSL)을 선택합니다.
   4. 외부 로그 유형 및 Traps ESM 버전에 대해 Traps_ESM을 선택합니다. 예를 들어 Traps ESM 4.0 또는 4.1의 경우 **3.4.1+**를 선택합니다.

      Traps 로그 형식이 업데이트되면 Panorama의 콘텐츠 업데이트를 통해 업데이트된 로그 정의를 사용할 수 있습니다.
4. **Panorama** > 수집기 그룹 > 로그 수집을 선택한 다음 수집기 그룹이 프로파일에 나열된 ESM 서버에서 로그를 수신할 수 있도록 로그 수집 프로파일 추가를 선택합니다.

   Panorama와 ESM Server 간의 보안 syslog 통신을 위해 SSL을 활성화하는 경우, Collector Group(**Panorama** > 관리형 수집기 > **General**)에 속하는 관리형 수집기에 인증서를 연결하고 보안 시스템 로그을 위한 인바운드 인증서에 사용할 인증서를 선택해야 합니다.
5. Panorama 및 Collector Group에 대한 변경 사항을 커밋합니다.

STEP 2 | ESM 서버에서 Panorama를 Syslog 수신기로 구성합니다.

Traps ESM 4.0 이상은 외부 syslog 수신기와 Panorama 모두에 대한 로그 포워딩을 지원합니다. 이전 Traps ESM 버전는 여러 syslog 수신기에 대한 로그 포워딩을 지원하지 않으므로 **Syslog** 설정에서

 ©2024 Palo Alto Networks, Inc.

Panorama를 syslog 수신기로 구성해야 합니다(Traps ESM 3.4의 경우 외부 로깅 플랫폼으로 로그 포워딩 활성화 참조).

Traps ESM 4.0 이상 버전의 경우:

1. ESM 콘솔에서 설정 > **ESM** > **Panorama**를 선택한 다음 **Panorama**로 로그 포워딩 활성화를 선택합니다.
2. Panorama 호스트 이름 또는 IP 주소를 **Panorama Server**로 입력하고 Panorama가 수신 대기 중인 **Panorama Server** 포트를 입력합니다. 선택적 **Panorama** 페일오버 서버에 대해 이 단계를 반복합니다.
3. 전송 계층 통신 프로토콜 선택: TCP, SSL이 있는 TCP 또는 UDP. SSL을 사용하는 TCP를 선택하는 경우 ESM 서버는 클라이언트 인증을 활성화하기 위해 서버 인증서가 필요합니다.

   Panorama에서 Secure Syslog용 인바운드 인증서에 대한 루트 CA 인증서를 내보내고 ESM 서버를 설치한 호스트의 신뢰할 수 있는 루트 인증서 저장소로 인증서를 가져와야 합니다.

STEP 3 | ESM 로그 및 상관 이벤트를 봅니다.

1. 모니터 > 외부 로그 > 트랩 **ESM**을 선택하여 Panorama에 수집된 로그를 봅니다.
2. 모니터 > 자동화된 상관 관계 엔진 > 상관 이벤트를 선택한 다음 **Wildfire** 및 트랩 **ESM** 상관 **C2** 상관 개체 이름을 필터링하여 상관 이벤트를 찾습니다. Panorama는 네트워크의 호스트가 WildFire 가상 환경에서 악성 파일에 대해 관찰된 동작과 일치하는 명령 및 제어 활동을 나타낼 때 상관 이벤트를 생성합니다. 이 상관 이벤트는 Traps 에이전트와 방화벽이 네트워크에 있는 하나 이상의 감염된 호스트에서 관찰한 의심스러운 활동에 대해 경고합니다.

 ©2024 Palo Alto Networks, Inc.

사용 사례: Panorama를 사용하여 애플리케이션 모니터링

이 예에서는 현재 정책의 효율성을 평가하고 네트워크에 대한 허용 가능한 사용 정책을 강화하기 위해 정책을 조정해야 하는 위치를 결정하는 프로세스를 안내합니다.

Panorama에 로그인하면 대시보드의 상위 애플리케이션 위젯에서 지난 1시간 동안 가장 많이 사용한 애플리케이션의 미리보기를 제공합니다. 위젯을 표시하려면 도구 모음에서 **Widgets** > **Application** > 상위 애플리케이션을 선택하십시오. 상위 애플리케이션 목록을 한 눈에 살펴보고 세부 정보를 검토하려는 각 애플리케이션 블록에 마우스를 올리거나 **ACC** 탭을 선택하여 정렬된 목록과 동일한 정보를 볼 수 있습니다. 다음 이미지는 대시보드의 상위 애플리케이션 위젯 보기입니다.

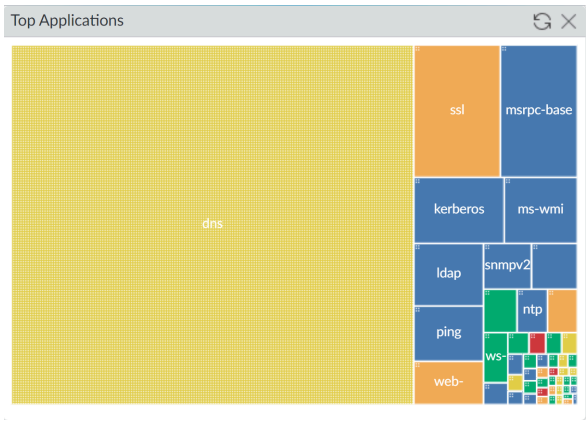


그림 **25:** 상위 애플리케이션 위젯

이 디스플레이의 데이터 소스는 애플리케이션 통계 데이터베이스입니다. 트래픽 로그를 사용하지 않으며 보안 규칙에 대한 로깅을 활성화했는지의 여부와 관계없이 생성됩니다. 네트워크의 트래픽에 대한 이 보기는 네트워크에서 허용되고 정의한 정책 규칙에 의해 차단되지 않은 상태로 흐르는 모든 것을 보여줍니다.

ACC 탭에서 데이터 소스를 선택한 다음 **Panorama**에서 로컬로 전환하거나 데이터에 대해 관리되는 방화벽(원격 디바이스 데이터)을 쿼리할 수 있습니다. Panorama는 자동으로 정보를 집계하고 표시합니다. 관리 방화벽에서 데이터를 로드하는 시간은 데이터를 보기로 선택한 기간과 네트워크에 생성된 트래픽 양에 따라 달라지므로 보다 빠른 흐름을 위해 Panorama를 데이터 원본으로 사용하는 것을 고려하십시오(Panorama로의 로그 포워딩 활성화). 관리 방화벽에 PAN-OS 7.0 및 이전 버전의 조합이 있는 경우 원격 디바이스 데이터를 사용할 수 없습니다.

Figure 1의 대시보드 예는 DNS를 인기 있는 애플리케이션으로 보여줍니다. DNS 애플리케이션 블록을 클릭하면 Panorama는 DNS가 전역 필터로 적용된 **ACC** > **Network Activity** 탭을 열고 애플리케이션에 대한 정보, 애플리케이션에 액세스한 사용자, 애플리케이션의 위험 수준 및 특성에 대한 세부 정보를 표시합니다.

©2024 Palo Alto Networks, Inc.

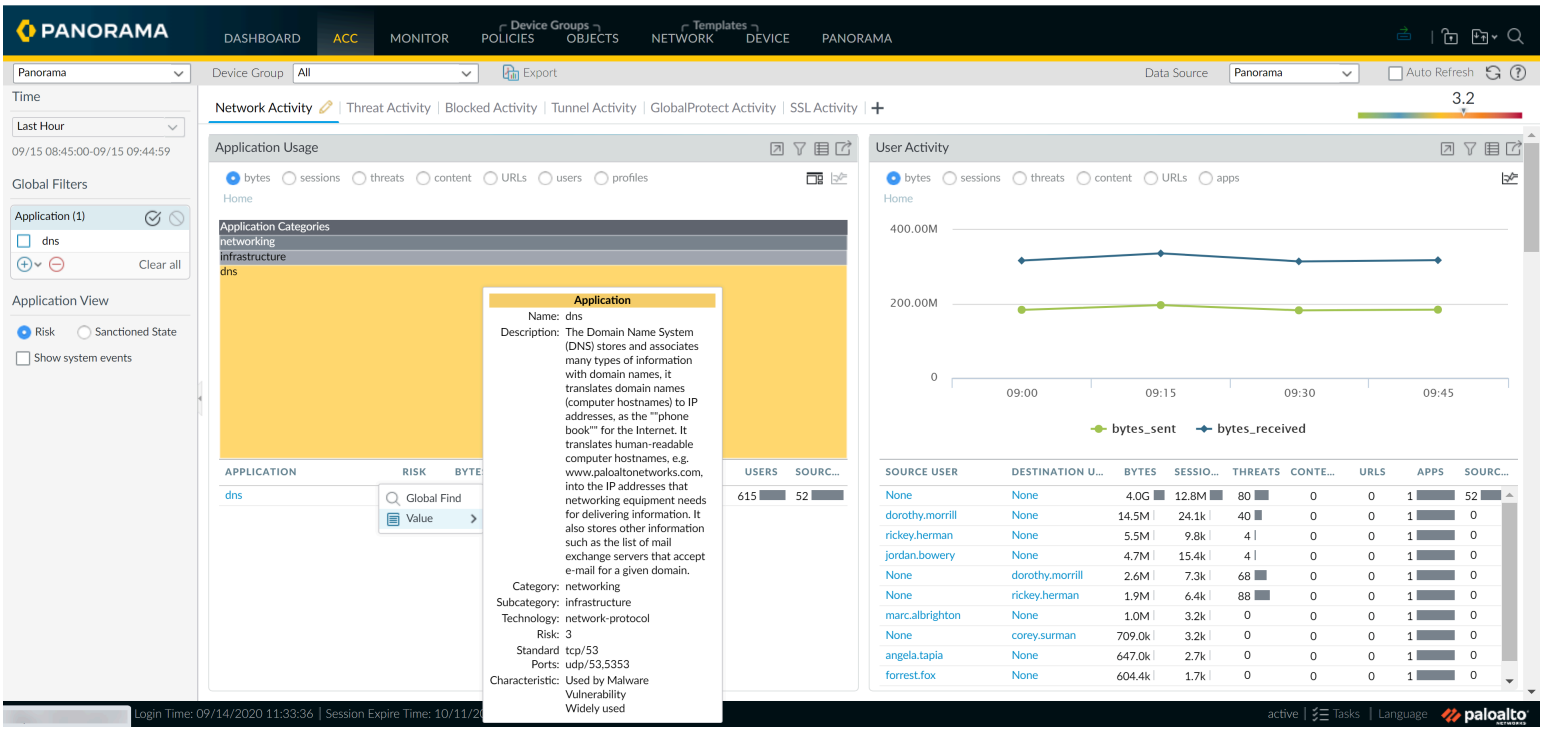


그림 **26:** 네트워크 활동 탭

사용자 활동 위젯에서 DNS를 사용 중인 사용자 수와 생성되는 트래픽 양을 확인할 수 있습니다. User-ID를 활성화한 경우 이 트래픽을 생성하는 사용자의 이름을 보고 드릴 인하여 각 사용자와 관련된 모든 세션, 콘텐츠 또는 위협을 검토할 수 있습니다.

위협 활동 탭에서 손상된 호스트 위젯을 보고 어떤 상관 관계 개체가 일치했는지 확인하고 사용자 및 애플리케이션과 관련된 일치 증거를 확인합니다. 위협 활동 위젯에서 위협 이름, 카테고리 및 ID를 볼 수도 있습니다.

DNS가 전역 필터로 설정된 상태에서 대상 **IP** 활동 및 대상 지역 위젯을 사용하여 트래픽의 대상 위치를 확인합니다. 또한 수신 및 송신 영역과 이 연결을 허용하는 보안 규칙을 볼 수 있습니다.

자세한 정보를 보려면 필터링된 보기에 대한 트래픽 로그로 이동하고 사용된 포트, 전송된 패킷, 전송 및 수신된 바이트에 대한 각 로그 항목을 검토하십시오. 열을 조정하여 필요에 따라 더 많은 정보를 보거나 더 적은 정보를 봅니다.

Monitor > **App-Scope** > 트래픽 맵 탭은 트래픽 플로우의 지리적 맵을 표시하고 들어오는 트래픽과 나가는 트래픽의 보기를 제공합니다. 모니터 > 앱 범위 > 모니터 변경 탭을 사용하여 트래픽 패턴의 변경 사항을 볼 수도 있습니다. 예를 들어, 이 시간 동안 가장 많이 사용된 애플리케이션을 지난 주 또는 달과 비교하여 패턴이나 추세가 있는지 확인합니다.

이제 발견한 모든 정보를 사용하여 정책 구성에 적용할 변경 사항을 평가할 수 있습니다. 다음은 고려해야 할 몇 가지 제안 사항입니다.

- 모든 DNS 트래픽을 차단하거나 허용하도록 제한하고 Panorama에서 사전 규칙을 만드십시오. 그런 다음 Panorama 디바이스 그룹을 사용하여 이 정책 규칙을 생성하고 하나 이상의 방화벽에 푸시합니다.
- 대역폭 사용 제한을 적용하고 비업무 트래픽의 우선 순위를 낮추는 QoS 프로파일 및 정책 규칙을 생성합니다. Panorama 디바이스 그룹 및 템플릿을 사용하여 QoS를 구성한 다음 규칙을 하나 이상의 방화벽에 푸시합니다.

©2024 Palo Alto Networks, Inc.

- 특정 사용자의 활동과 네트워크에서 사용되는 상위 애플리케이션의 활동을 모아서 조치를 취하기 전에 1~2주 동안 해당 패턴을 관찰하는 사용자 정의 보고서 그룹을 예약하십시오.

특정 애플리케이션을 확인하는 것 외에도 상위 애플리케이션 목록에서 알 수 없는 애플리케이션을 확인할 수도 있습니다. 정의된 App-ID™ 서명과 일치하지 않고 unknown-udp 및 unknown-tcp로 표시되는 애플리케이션입니다. 이러한 알 수 없는 애플리케이션에 대해 자세히 알아보려면 이름을 클릭하여 분류되지 않은 트래픽에 대한 세부 정보로 드릴다운하십시오.

동일한 프로세스를 사용하여 세션이 설정된 대상 호스트의 IP 주소와 함께 알 수 없는 트래픽을 시작한 호스트의 최상위 소스 IP 주소를 조사합니다. 알 수 없는 트래픽의 경우 트래픽 로그는 기본적으로 알 수 없는 애플리케이션이 감지될 때 패킷 캡처(pcap)를 수행합니다. 왼쪽 열의 녹색 화살표는 애플리케이션 데이터의 패킷 캡처 스니펫을 나타냅니다. 녹색 화살표를 클릭하면 브라우저에 pcap이 표시됩니다.

서버의 IP 주소(대상 IP), 대상 포트 및 패킷 캡처가 있으면 애플리케이션을 식별하고 네트워크에서 조치를 취하는 방법을 결정하는 데 더 유리합니다. 예를 들어 알 수 없는 TCP 또는 UDP 트래픽으로 레이블을 지정하는 대신 이 트래픽을 식별하는 사용자 지정 애플리케이션을 만들 수 있습니다. 알 수 없는 애플리케이션 식별에 대한 자세한 내용은 알 수 없는 애플리케이션 식별 문서를 참조하고 애플리케이션 식별을 위한 사용자 지정 서명 개발에 대한 정보는 사용자 지정 애플리케이션 서명 문서를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

사용 사례: Panorama를 사용하여 사고에 대응

네트워크 위협은 드라이브 바이 다운로드로 인한 멀웨어 및 스파이웨어 감염, 피싱 공격, 패치되지 않은 서버, 무작위 또는 표적 서비스 거부(DoS) 공격 등 다양한 벡터에서 시작될 수 있습니다. 네트워크 공격이나 감염에 대응할 수 있으려면 관리자에게 공격을 경고하고 공격을 시작하는 데 사용된 소스와 방법을 추적하는 데 필요한 포렌식 증거를 제공하는 프로세스와 시스템이 필요합니다.

Panorama가 제공하는 이점은 네트워크를 통해 관리되는 방화벽에서 수집된 패턴 및 로그에 대한 중앙 집중식 통합 보기입니다. 자동화된 상관 관계 엔진의 정보를 단독으로 사용하거나 SIEM(Security Information Event Manager)에서 생성된 보고서 및 로그와 함께 사용하여 공격이 트리거된 방법과 향후 공격 및 네트워크 손상을 방지하는 방법을 조사할 수 있습니다.

이 사용 사례가 조사하는 질문은 다음과 같습니다.

- 사건에 대한 알림은 어떻게 받습니까?
- 사건이 거짓 긍정이 아니라는 것을 어떻게 확증합니까?
- 즉각적인 조치는 무엇입니까?
- 사용 가능한 정보를 사용하여 트리거 이벤트 이전 또는 이후의 이벤트 시퀀스를 재구성하는 방법은 무엇입니까?
- 네트워크 보안을 위해 고려해야 할 변경 사항은 무엇입니까?

이 사용 사례는 특정 사건을 추적하고 Panorama의 가시성 도구가 보고서에 대응하는 데 어떻게 도움이 되는지 보여줍니다.

- 사고 알림
- ACC의 위젯 검토
- 위협 로그 검토
- WildFire 로그 검토
- 데이터 필터링 로그 검토
- 보안 규칙 업데이트

사고 알림

Palo Alto Networks 방화벽을 구성한 방법과 추가 분석에 사용할 수 있는 타사 도구에 따라 사고에 대해 경고를 받을 수 있는 몇 가지 방법이 있습니다. Panorama 또는 syslog 서버에 기록된 로그 항목에 의해 트리거된 이메일 알림을 받거나, SIEM 솔루션에서 생성된 전문 보고서를 통해 알림을 받을 수 있으며, 타사 유료 서비스 또는 에이전시에서 알림을 받을 수 있습니다. 이 예에서는 Panorama에서 이메일 알림을 수신한다고 가정해 보겠습니다. 이메일은 스파이웨어 서명과 일치하는 Zero Access gent.Gen 명령 및 제어 트래픽에 대한 경고에 의해 트리거된 이벤트를 알려줍니다. 또한 이메일에는 세션의 소스 및 대상 IP 주소, 위협 ID 및 이벤트가 기록된 타임스탬프가 나열됩니다.

 ©2024 Palo Alto Networks, Inc.

ACC의 위젯 검토

ACC > 위협 활동 탭에서 손상된 호스트 위젯 및 위협 활동 위젯을 확인하여 심각도 또는 높은 심각도 위협이 있는지 확인합니다. 손상된 호스트 위젯에서 일치하는 개체를 살펴보고 일치 횟수 값을 클릭하여 관련 인시던트에 대한 일치 증거를 확인합니다.

위협 로그 검토

경보 조사를 시작하려면 위협 ID를 사용하여 Panorama(**Monitor** > **Logs** > **Threat**)에서 위협 로그를 검색하십시오. 위협 로그에서 피해자의 IP 주소를 찾고, 로그 항목에서 다운로드 아이콘 을 클릭하여 패킷 캡처(PCAP)를 내보내고, WireShark와 같은 네트워크 분석 도구를 사용하여 패킷 세부 정보를 검토할 수 있습니다. HTTP의 경우 프로토콜, 의심스러운 호스트, URL 문자열, 사용자 에이전트, IP 주소 및 포트에서 잘못된 형식 또는 가짜 HTTP REFERER를 찾아 사건을 확인합니다. 이러한 pcap의 데이터는 유사한 데이터 패턴을 검색하고 사용자 지정 서명을 생성하거나 보안 정책을 수정하여 향후 위협에 더 잘 대처할 때도 유용합니다.

이 수동 검토의 결과 서명에 대해 확신이 든다면 서명을 경고 작업에서 차단 작업으로 전환하여 보다 적극적인 접근 방식을 고려하십시오. 경우에 따라 해당 IP 주소의 추가 트래픽이 내부 네트워크에 도달하지 못하도록 공격자 IP를 IP 차단 목록에 추가하도록 선택할 수 있습니다.

DNS 기반 스파이웨어 서명이 보이면 로컬 *DNS* 서버의 *IP* 주소가 피해자 ***IP*** 주소로 표시될 수 있습니다. 이는 방화벽이 로컬 *DNS* 서버의 북쪽에 있기 때문에 *DNS* 쿼리가 요청을 보낸 클라이언트의 *IP* 주소를 표시하는 대신 로컬 *DNS* 서버를 소스 *IP*로 표시하기 때문인 경우가 많습니다.

이 문제가 표시되면 보안 규칙의 안티 스파이웨어 프로파일에서 *DNS* 싱크홀링 작업을 활성화하여 네트워크에서 감염된 호스트를 식별합니다. *DNS* 싱크홀링을 사용하면 악의적인 도메인에 대한 아웃바운드 연결을 제어하고 *DNS* 쿼리를 사용되지 않는 내부 *IP* 주소로 리디렉션할 수 있으며, 싱크홀을 통한 대응이 도출되지 않습니다. 손상된 호스트가 악의적인 도메인에 대한 연결을 시작하면 인터넷으로 나가는 대신 방화벽이 사용자가 정의한 *IP* 주소로 요청을 리디렉션하고 싱크홀됩니다. 이제 싱크홀에 연결된 모든 호스트의 트래픽 로그를 검토하면 감염된 모든 호스트를 찾고 확산을 방지하기 위한 교정 조치를 취할 수 있습니다.

사건에 대한 조사를 계속하려면 공격자 및 피해자 IP 주소에 대한 정보를 사용하여 다음과 같은 추가 정보를 찾으십시오.

- 공격자는 지리적으로 어디에 있습니까? IP 주소는 개별 IP 주소입니까 아니면 NAT된 IP 주소입니까?
- 사용자가 속아서 웹사이트로 이동하거나 다운로드하여 이벤트가 발생했습니까? 아니면 이메일 첨부 파일을 통해 전송되었습니까?
- 악성코드가 전파되고 있습니까? 네트워크에 다른 손상된 호스트/엔드포인트가 있습니까?
- 제로데이 취약점에 해당합니까?

각 로그 항목에 대한 로그 세부 정보에는 이벤트에 대한 관련 로그가 표시됩니다. 이 정보는 사고로 이어진 이벤트를 검토하고 상호 연관시킬 수 있는 트래픽, 위협, URL 필터링 또는 기타 로그를 알려줍니다. 예를 들어, IP 주소를 원본 및 대상 IP로 사용하여 트래픽 로그(**Monitor** > **Logs** > **Traffic**)를 필터링하여 이 피해자 IP 주소가 연결을 설정한 모든 외부 및 내부 호스트/클라이언트의 전체 그림을 얻습니다.

 ©2024 Palo Alto Networks, Inc.

WildFire 로그 검토

위협 로그 외에도 피해자 IP 주소를 사용하여 WildFire 제출 로그를 필터링합니다. WildFire 제출 로그에는 분석을 위해 WildFire 서비스에 업로드된 파일에 대한 정보가 포함되어 있습니다. 스파이웨어는 일반적으로 은밀하게 내장되기 때문에 WildFire 제출 로그를 검토하면 피해자가 최근에 의심스러운 파일을 다운로드했는지의 여부를 알 수 있습니다. WildFire 포렌식 보고서는 파일 또는 .exe를 불러온 URL 및 콘텐츠 동작에 대한 정보를 표시합니다. 파일이 악성인지, 레지스트리 키 수정, 파일 읽기/쓰기, 새 파일 생성, 네트워크 통신 채널 열기, 애플리케이션 충돌 유발, 프로세스 생성, 파일 다운로드 또는 기타 악의적인 동작을 보이는지 알려줍니다. 이 정보를 사용하여 감염을 일으킨 애플리케이션(웹 탐색, SMTP, FTP)을 차단할지, URL 필터링 규칙을 더 엄격하게 만들지, 일부 애플리케이션/작업을 제한할지(예: 특정 사용자 그룹에 대한 파일 다운로드)를 결정합니다.

*Panorama*에서 *WildFire* 로그에 액세스하려면 *WildFire* 구독, 보안 규칙에 연결된 파일 차단 프로파일 및 *Panorama*로 위협 로그 포워딩이 필요합니다.

*Panorama*가 *PAN-OS 7.0* 이전 버전의 소프트웨어를 실행하는 방화벽을 관리할 경우 *Panorama*가 해당 방화벽이 제출하는 *WildFire* 샘플에 대한 분석 정보를 수집할 수 있는 *WildFire* 서버를 지정하십시오. *Panorama*는 이 정보를 사용하여 *PAN-OS 7.0*에 도입된 필드 값이 누락된 *WildFire* 제출 로그를 완성합니다. 이전 릴리스를 실행하는 방화벽은 해당 필드를 채우지 않습니다. 서버를 지정하려면 ***Panorama*** > ***Setup*** > ***WildFire***를 선택한 다음 일반 설정을 편집한 다음 ***WildFire Private Cloud*** 이름을 입력합니다. 기본값은 미국에서 호스팅되는 *WildFire* 클라우드인 ***wildfire-public-cloud***입니다.

WildFire에서 파일이 악성이라고 판단하면 24-48시간 이내에 새로운 안티바이러스 서명이 생성되어 사용할 수 있게 됩니다. WildFire 구독이 있는 경우 다음 WildFire 서명 업데이트의 일부로 30-60분 이내에 서명을 사용할 수 있습니다. Palo Alto Networks 차세대 방화벽이 이에 대한 서명을 수신하는 즉시 구성이 맬웨어를 차단하도록 구성된 경우 파일이 차단되고 차단된 파일에 대한 정보가 위협 로그에 표시됩니다. 이 프로세스는 긴밀하게 통합되어 이 위협으로부터 사용자를 보호하고 네트워크에서 맬웨어의 확산을 방지합니다.

데이터 필터링 로그 검토

데이터 필터링 로그(**Monitor** > **Logs** > **Data Filtering**)는 악성 네트워크 활동을 조사하기 위한 또 다른 귀중한 소스입니다. 경고를 받고 있는 모든 파일에 대한 로그를 주기적으로 검토할 수 있지만 로그를 사용하여 피해자 IP 주소 또는 사용자와의 파일 및 데이터 전송을 추적하고, 서버에서 클라이언트로 또는 클라이언트에서 서버로의 트래픽 방향과 흐름을 확인할 수도 있습니다. 이벤트 전후의 이벤트를 다시 생성하려면 대상 IP 주소에 대한 로그를 필터링하고 네트워크 활동에 대한 로그를 검토하십시오.

Panorama는 관리되는 모든 방화벽의 정보를 집계하기 때문에 네트워크의 모든 활동에 대한 좋은 개요를 제공합니다. 네트워크의 트래픽을 조사하는 데 사용할 수 있는 다른 시각적 도구로는 **Threat Map**, **Traffic Map** 및 **Threat Monitor**가 있습니다. 위협 맵 및 트래픽 맵(**Monitor** > **AppScope** > **Threat** 맵 또는 트래픽 맵)을 사용하면 수신 및 발신 트래픽에 대한 지리적 영역을 시각화할 수 있습니다. DDoS 공격과 같이 외부에서 발생할 수 있는 공격을 나타낼 수 있는 비정상적인 활동을 볼 때 특히 유용합니다. 예를 들어, 동유럽과의 비즈니스 거래가 많지 않고 지도에 해당 지역의 비정상적인 트래픽 수준이 표시되면 지도의 해당 영역을 클릭하여 상위 애플리케이션에서의 ACC 정보, 세션 수의 트래픽 세부사항, 전송 및 수신된 바이트, 상위 소스 및 대상, 사용자 또는 IP 주소, 탐지된 위협의 심각도(있는 경우)에 대한 세부 정보를 실행하고 확

 ©2024 Palo Alto Networks, Inc.

인할 수 있습니다. 위협 모니터(**Monitor** > **AppScope** > **Threat Monitor**)는 네트워크의 상위 10개 위협 또는 네트워크의 상위 공격자 또는 상위 피해자 목록을 표시합니다.

보안 규칙 업데이트

이제 발견한 모든 정보를 통해 위협이 네트워크에 미치는 영향(공격 규모, 소스, 손상된 호스트, 위험 요소)을 함께 스케치하고 후속 조치를 위해 어떤 변경 사항이 있는지 평가할 수 있습니다. 다음은 고려해야 할 몇 가지 제안 사항입니다.

- 임의의 조기 삭제를 구성하거나 TCP 플러드에 대한 SYN 쿠키를 삭제하도록 DoS 보호 프로파일을 향상하여 DDoS 공격을 방지합니다. ICMP 및 UDP 트래픽에 제한을 두는 것이 좋습니다. 로그에서 발견한 추세와 패턴을 기반으로 사용 가능한 옵션을 평가하고 Panorama 템플릿을 사용하여 변경 사항을 구현합니다.

  동적 차단 목록(객체 > 동적 차단 목록)을 만들어 자체 위협 로그 분석, 특정 IP 주소의 DDoS 공격 또는 타사 IP 차단 목록과 같은 여러 인텔리전스 소스에서 발견한 특정 IP 주소를 차단합니다.

  목록은 웹 서버에 있는 텍스트 파일이어야 합니다. Panorama의 디바이스 그룹을 사용하여 방화벽이 웹 서버에 액세스하고 정의된 빈도로 목록을 가져올 수 있도록 개체를 관리되는 방화벽으로 푸시합니다. 동적 차단 목록 개체를 생성한 후 소스 및 대상 필드의 주소 개체를 사용하여 정의된 IP 주소, 범위 또는 서브넷에서 들어오고 나가는 트래픽을 차단하는 보안 규칙을 정의합니다. 이 접근 방식을 사용하면 문제를 해결하고 네트워크 보안을 위해 더 큰 정책 변경을 수행할 때까지 침입자를 차단할 수 있습니다.
- 감염을 일으킨 특정 애플리케이션(웹 브라우징, SMTP, FTP)을 차단하기 위해 공유 정책 규칙 또는 디바이스 그룹 규칙을 생성할지, 보다 엄격한 URL 필터링 규칙을 만들지, 또는 일부 애플리케이션/동작을 제한할지 결정합니다(예: 특정 사용자 그룹을 대상으로 파일 다운로드).
- Panorama에서는 방화벽 컨텍스트로 전환하고 네트워크에서 잠재적인 봇넷 감염 호스트를 식별하는 봇넷 보고서에 대한 방화벽을 구성할 수도 있습니다.

 ©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

Panorama 고가용성

시스템 또는 네트워크 장애 시 이중화를 제공하기 위해 두 개의 Panorama™ 관리 서버를 고가용성(HA) 구성으로 배포할 수 있습니다. Panorama는 한 피어가 활성-기본이고 다른 피어가 수동-보조인 HA 구성을 지원합니다. 기본 피어에서 장애가 발생하면 자동으로 페일오버되고 보조 피어가 활성화됩니다.

- Panorama HA 전제 조건
- HA의 Panorama에 대한 우선 순위 및 페일오버
- 페일오버 트리거
- Panorama HA의 로깅 고려 사항
- Panorama HA 피어 간의 동기화
- Panorama HA 쌍 관리

Panorama HA 전제 조건

HA에서 Panorama를 구성하려면 각각에 대해 다음 요구 사항이 있는 동일한 Panorama 서버 쌍이 필요합니다.

- 동일한 폼 팩터 - 피어는 동일한 모델이어야 합니다. 그러한 모델은 두 M-700 어플라이언스, 두 M-600 어플라이언스, 두 M-500 어플라이언스, 두 M-300 어플라이언스, 두 M-200 어플라이언스이거나 둘 다 Panorama 가상 어플라이언스에 대해 지원되는 동일한 하이퍼바이저에 배포됩니다. 예를 들어 Panorama 모드에서 AWS에 배포된 Panorama 가상 어플라이언스에 대한 HA를 성공적으로 구성하려면 HA 피어도 AWS에 배포되고 Panorama 모드에 있어야 합니다.
- 동일한 모드 - 피어는 동일한 Panorama 모드에 있어야 합니다. 둘 다 Panorama 모드, 관리 전용 모드 또는 레거시 모드(ESXi 및 vCloud Air만 해당)에서 실행됩니다.

  Log Collector 모드의 Panorama 어플라이언스는 HA를 지원하지 않습니다.
- 동일한 **Panorama OS** 버전 - 구성 정보를 동기화하고 원활한 페일오버를 위해 패리티를 유지하려면 동일한 Panorama 버전을 실행해야 합니다.
- 동일한 라이선스 세트 - 동일한 방화벽 관리 용량 라이선스가 있어야 합니다.
- (Panorama 가상 어플라이언스만 해당) **FIPCS-CC** 모드 - 두 Panorama HA 피어에서 FIPS-CC 모드를 활성화하거나 비활성화해야 합니다.
- (Panorama 가상 어플라이언스만 해당) 가상 어플라이언스 리소스 - 구성 정보를 성공적으로 동기화하려면 동일한 수의 vCPU 코어와 메모리가 할당되어야 합니다.
- (Panorama 가상 어플라이언스만 해당) 고유한 일련번호 - 고유한 일련번호가 있어야 합니다. 두 Panorama 인스턴스의 일련번호가 동일한 경우 문제를 해결할 때까지 일시 중단 모드로 유지됩니다.

Panorama HA 피어 간에 로깅 디스크 수와 로깅 디스크 용량을 일치시키는 것이 권장되지만 *Panorama HA* 피어 간에 로깅 디스크 수 또는 로깅 디스크 용량이 달라도 구성 동기화 또는 *HA* 페일오버에 영향을 미치지 않습니다

.

©2024 Palo Alto Networks, Inc.

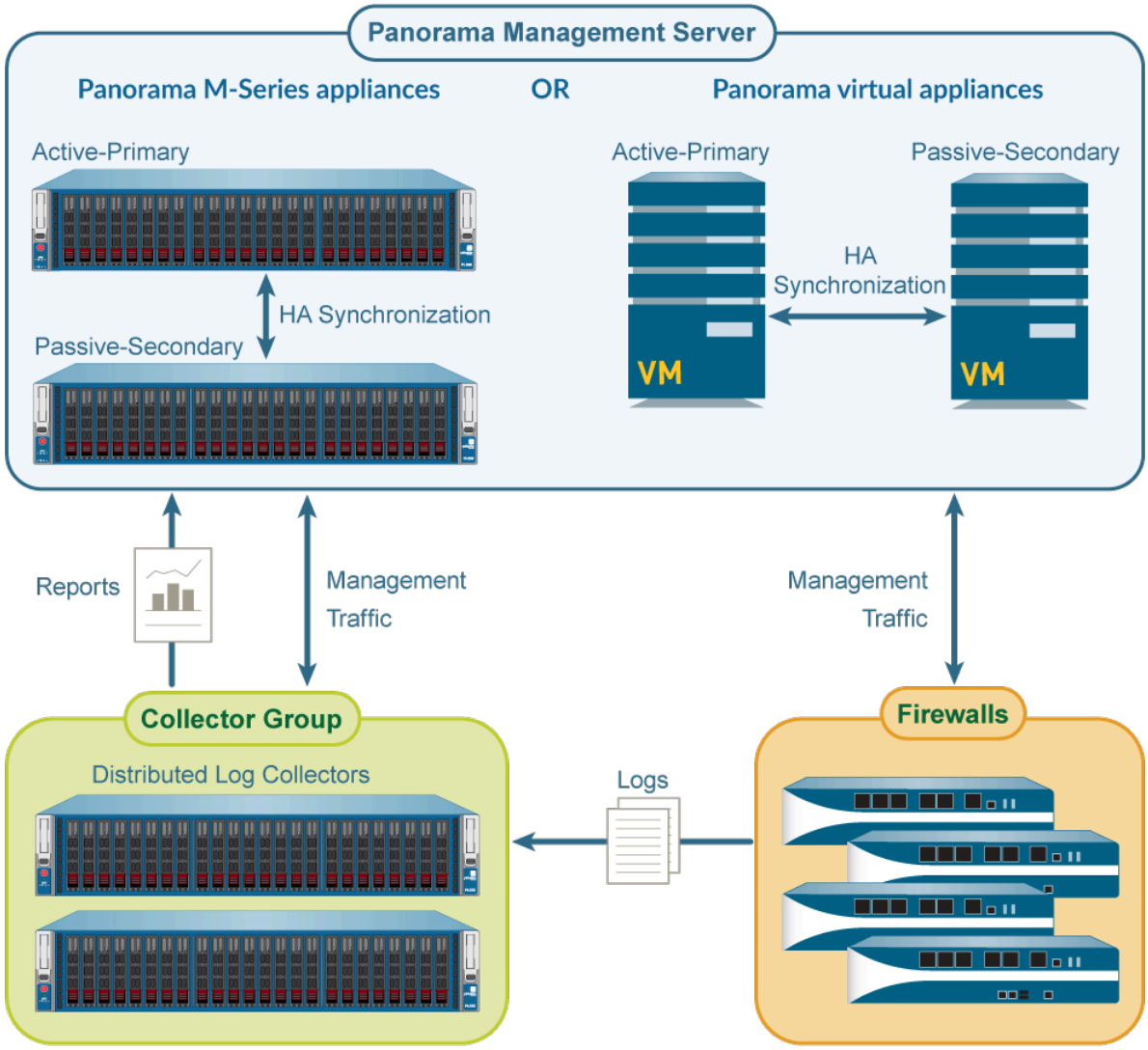


그림 **27: Panorama HA** 조직

HA 구성의 Panorama 서버는 피어이며 몇 가지 예외(Panorama HA 피어 간 동기화 참조)를 제외하고 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터를 중앙에서 관리하기 위해 활성 또는 수동 중 하나를 사용할 수 있습니다. HA 피어는 관리(MGT) 인터페이스를 사용하여 관리 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터에 푸시된 구성 요소를 동기화하여 상태 정보를 유지합니다. 일반적으로 Panorama HA 피어는 지리적으로 다른 사이트에 있으므로 각 피어에 할당된 MGT 인터페이스 IP 주소가 네트워크를 통해 라우팅할 수 있는지 확인해야 합니다. HA 연결은 암호화가 활성화된 TCP 포트 28을 사용합니다. 암호화가 활성화되지 않은 경우 포트 28769 및 28260은 HA 연결 및 HA 피어 간의 구성 동기화에 사용됩니다. 피어 간의 지연 시간은 500ms 미만을 권장합니다. 대기 시간을 확인하려면 정상 트래픽 기간 동안 Ping을 사용합니다.

*Palo Alto Networks*는 하나의 로그 수집기에 액세스할 수 없게 되면 수집기 그룹이 작동하지 않게 되는 것을 방지하기 위해 수집기 그룹에 최소 *3*개의 로그 수집기를 추가할 것을 권장합니다. 자세한 내용은 수집기 그룹의 기본 동작 변경을 참조하십시오.

©2024 Palo Alto Networks, Inc.

HA의 Panorama에 대한 우선 순위 및 페일오버

HA 쌍의 각 Panorama 피어에는 우선 순위 값이 할당됩니다. 1차 또는 2차 피어의 우선 순위 값은 관리 및 로그 관리의 주요 지점이 될 자격이 있는 피어를 결정합니다. 기본으로 설정된 피어는 활성 상태를 가정하고 보조는 수동이 됩니다. 활성 피어는 모든 구성 변경 사항을 처리하고 관리되는 방화벽으로 푸시합니다. 수동 피어는 구성을 변경하거나 관리 방화벽에 구성을 푸시할 수 없습니다. 그러나 두 피어 중 하나를 사용하여 보고서를 실행하거나 로그 쿼리를 수행할 수 있습니다.

패시브 피어는 동기화되어 활성 Panorama에서 경로, 링크, 시스템 또는 네트워크 장애가 발생할 경우 활성 상태로 전환할 준비가 됩니다.

페일오버가 발생하면 Panorama 피어의 상태(활성 또는 수동)만 변경됩니다. 우선 순위(1차 및 2차)는 그렇지 않습니다. 예를 들어, 기본 피어가 실패하면 상태가 활성-기본에서 수동-기본으로 변경됩니다.

활성-보조 상태의 피어는 두 가지 예외를 제외하고 모든 기능을 수행할 수 있습니다.

- 라이선스 업데이트 또는 소프트웨어 업그레이드와 같은 방화벽 또는 Log Collector 배포 기능을 관리할 수 없습니다.
- 우선 순위를 기본으로 수동으로 변경할 때까지 NFS에 기록할 수 없습니다. 레거시 모드의 Panorama 가상 어플라이언스만 NFS를 지원합니다.

다음 표에는 상태 및 우선 순위 설정에 따른 Panorama의 기능이 나열되어 있습니다.

Capability	active-primary	passive-primary passive-secondary	active-secondary
Switch device context	■	■	■
Perform distributed reporting	■	■	■
Manage shared policy	■	■	■
Log to local disk	■	■ (Optional on the Panorama virtual appliance only)	■ (Optional on the Panorama virtual appliance only)
Log to an NFS partition (Panorama virtual appliance only)	■	■	■
Deploy software and licenses	■	■	■
Export Panorama configuration	■	■	■

그림 **28: Panorama HA** 기능

자세한 내용은 Panorama HA 전제 조건 또는 Panorama에서 HA 설정을(를) 참조하십시오.

©2024 Palo Alto Networks, Inc.

페일오버 트리거

활성 Panorama에서 장애가 발생하고 수동 Panorama가 방화벽 관리 작업을 인계받는 경우 이벤트를 페일오버(failover)라고 합니다. 활성 Panorama에서 모니터링되는 메트릭이 실패하면 페일오버가 트리거됩니다. 이 실패는 기본 Panorama의 상태를 활성-기본에서 수동-기본으로 전환하고 보조 Panorama는 활성-보조가 됩니다.

페일오버를 트리거하는 조건은 다음과 같습니다.

- Panorama 피어는 서로 통신할 수 없으며 활성 피어는 상태 및 상태 폴링에 응답하지 않습니다. 사용된 메트릭은 HA 하트비트 폴링 및 Hello 메시지입니다.

  Panorama 피어가 서로 통신할 수 없는 경우 활성 피어는 페일오버가 트리거되기 전에 피어가 현재 연결되어 있는지 모니터링합니다. 이 검사는 페일오버를 피하고 두 Panorama 피어가 모두 활성 상태인 분할 브레인 시나리오를 유발하는 데 도움이 됩니다.
- 활성 피어에 지정된 하나 이상의 대상(IP 주소)에 연결할 수 없습니다. 사용된 메트릭은 HA 경로 모니터링입니다.

위에 나열된 페일오버 트리거 외에도 관리자가 Panorama 피어를 일시 중단된 상태로 두거나 선점이 발생할 때 페일오버가 발생합니다. 선점은 기본 Panorama가 장애(또는 사용자 개시 일시 중단)에서 복구한 후 활성 역할을 재개하는 기본 설정입니다. 기본적으로 선점은 활성화되어 있으며 기본 Panorama가 장애에서 복구되어 사용할 수 있게 되면 보조 Panorama가 제어를 포기하고 수동 상태로 돌아갑니다. 선점이 발생하면 이벤트가 시스템 로그에 기록됩니다.

NFS 데이터 저장소에 로깅하는 경우 기본 피어(NFS에 마운트된)가 활성 역할을 재개하고 NFS 데이터 저장소에 쓸 수 있도록 허용하므로 선점을 비활성화하지 마십시오. 다른 모든 배포의 경우 특정 Panorama가 기본 활성 피어인지 확인하려는 경우에만 선점이 필요합니다.

HA 하트비트 폴링 및 Hello 메시지

HA 피어는 Hello 메시지와 하트비트를 사용하여 피어가 응답하고 작동하는지 확인합니다. Hello 메시지는 다른 피어의 상태를 확인하기 위해 구성된 Hello 간격으로 한 피어에서 다른 피어로 전송됩니다. 하트비트는 HA 피어에 대한 ICMP 핑이며 피어는 핑에 응답하여 피어가 연결되고 응답하는지 확인합니다. 기본적으로 간격은 하트비트의 경우 1,000밀리초이고 Hello 메시지의 경우 8,000ms입니다.

HA 경로 모니터링

경로 모니터링은 IP 주소 또는 IP 주소 그룹(경로 그룹)에 대한 네트워크 연결 및 링크 상태를 확인합니다. 활성 피어는 ICMP 핑을 사용하여 하나 이상의 대상 IP 주소에 도달할 수 있는지 확인합니다. 예를 들어 라우터나 스위치와 같이 상호 연결된 네트워킹 디바이스의 가용성, 서버에 대한 연결 또는 트래픽 흐름에 있는 기타 중요한 디바이스의 가용성을 모니터링할 수 있습니다. 모니터링을 위해 구성된 노드/디바이스가 응답하지 않을 가능성이 있는지 확인합니다. 특히 부하가 발생하면 경로 모니터링 오류가 발생하고 페일오버가 트리거될 수 있습니다.

기본 핑 간격은 5,000ms입니다. 세 번의 연속 ping(기본값)이 실패하면 IP 주소에 연결할 수 없는 것으로 간주되고 모니터링되는 IP 주소 중 일부 또는 전체가 연결할 수 없게 되면 피어 오류가 트리거됩니다. 기본적으로 IP 주소 중 하나에 연결할 수 없으면 HA 상태가 작동하지 않음으로 전환됩니다.

©2024 Palo Alto Networks, Inc.

Panorama HA의 로깅 고려 사항

HA 구성에서 Panorama를 설정하면 로그 수집을 위한 중복성이 제공됩니다. 관리형 방화벽은 SSL을 통해 두 Panorama 피어에 연결되어 있으므로 상태 변경이 발생하면 각 Panorama는 관리형 방화벽에 메시지를 보냅니다. 방화벽은 Panorama HA 상태에 대한 알림을 받고 그에 따라 로그를 포워딩할 수 있습니다.

기본적으로 관리 방화벽이 *Panorama*에 연결할 수 없으면 로그를 버퍼링합니다. 연결이 복원되면 마지막으로 중단된 위치에서 로그 전송을 재개합니다.

하드웨어 기반 Panorama와 Panorama 가상 어플라이언스의 로깅 옵션은 다음과 같이 다릅니다.

- 레거시 모드에서 Panorama 가상 어플라이언스의 페일오버 로깅
- Panorama 모드의 M-시리즈 어플라이언스 또는 Panorama 가상 어플라이언스에서 페일오버 로깅

레거시 모드에서 Panorama 가상 어플라이언스의 페일오버 로깅

레거시 모드의 Panorama 가상 어플라이언스는 다음 로그 페일오버 옵션을 제공합니다.

로그 저장 유형	설명
가상 디스크	기본적으로 관리 방화벽은 각 Panorama HA 피어에 독립적인 스트림으로 로그를 보냅니다. 기본적으로 피어를 사용할 수 없게 되면 관리되는 방화벽이 로그를 버퍼링하고 피어가 다시 연결되면 중단된 위치에서 로그 전송을 재개합니다(디스크 저장 용량 및 연결 해제 기간에 따라 다름). 최대 로그 스토리지 용량은 가상 플랫폼(VMware ESXi 또는 vCloud Air)에 따라 다릅니다. 자세한 내용은 Panorama 모델을(를) 참조하십시오. 활성 피어에만 로그를 포워딩할지의 여부를 선택할 수 있습니다(로그 포워딩 및 버퍼링 기본값 수정 참조). 그러나 *Panorama*는 *HA* 쌍 전체에서 로그 집계를 지원하지 않습니다. 따라서 가상 디스크에 로그인하는 경우 모니터링 및 보고를 위해 관리 방화벽에서 로그를 수집하는 *Panorama* 피어를 쿼리해야 합니다.
네트워크 파일 시스템(NFS)	VMware ESXi 서버에서 실행되는 Panorama 가상 어플라이언스에만 NFS 스토리지를 마운트할 수 있습니다. 활성-기본 Panorama만 NFS 기반 로그 파티션에 마운트되고 로그를 수신할 수 있습니다. 페일오버 시 기본 디바이스는 수동-기본 상태가 됩니다. 이 시나리오에서 선점이 발생할 때까지 활성 보조 Panorama는 방화벽을 관리하지만 로그를 수신하지 않으며 NFS에 쓸 수 없습니다. 활성-보조 피어가 NFS에 로그인할 수 있도록 하려면 NFS 파티션에 마운트할 수 있도록 수동으로 기본 피어로 전환해야 합니다. 지침은 NFS 로깅을 재개하기 위해 Panorama 페일오버 후 우선 순위 전환을(를) 참조하십시오.

©2024 Palo Alto Networks, Inc.

Panorama 모드의 M-시리즈 어플라이언스 또는 Panorama 가상 어플라이언스에서 페일오버 로깅

M-700 어플라이언스, M-600 어플라이언스, M-500 어플라이언스, M-300 어플라이언스, M-200 어플라이언스 또는 Panorama 모드의 Panorama 가상 어플라이언스의 HA 쌍에 있는 로컬 로그 수집기로 방화벽 로그를 전달하는 경우 수집기 그룹을 구성할 때 어떤 방화벽이 어떤 로그 수집기로 로그를 보낼지 결정합니다. 각 Panorama 피어의 로그 수집기에 대해 별도의 수집기 그룹을 구성하거나 두 피어의 로그 수집기를 포함하도록 단일 수집기 그룹을 구성할 수 있습니다. 로컬 로그 수집기를 모두 포함하는 수집기 그룹에서 로그 포워딩 기본 설정 목록은 방화벽에서 로그를 수신하는 로그 수집기를 결정합니다. 모든 관리형 방화벽의 경우 수집기 그룹의 모든 로그 수집기에 로그를 보낼 수 있는 옵션이 있습니다. 이 경우 Panorama는 라운드 로빈 부하 분산을 사용하여 주어진 순간에 로그를 수신할 로그 수집기를 선택합니다.

로그 중복성을 활성화하여 각 로그에 사본이 있고 각 사본이 다른 로그 수집기에 있도록 할 수 있습니다. 이 중복성은 하나의 로그 수집기를 사용할 수 없게 되어도 로그가 손실되지 않도록 합니다. 수집기 그룹으로 포워딩된 모든 로그를 보고 모든 로그 정보에 대한 보고서를 실행할 수 있습니다. 로그 중복성은 Collector Group의 각 Log Collector에 동일한 수의 디스크가 있는 경우에만 사용할 수 있습니다.

로그 중복성을 활용하고 로깅 장애 조치를 보장하려면 수집기 그룹에 3개 이상의 로그 수집기를 추가하여 *PAN-OS 10.0*에 도입된 로그 수집기 *n/2+1* 쿼럼 요구 사항을 충족해야 합니다.

특정 수집기 그룹에 대한 모든 로그 수집기는 동일한 모델이어야 하며, 모든 *M-200* 어플라이언스, 모든 *M-300* 어플라이언스, 모든 *M-500* 어플라이언스, 모든 *M-600* 어플라이언스, 모든 *M-700* 어플라이언스 또는 모든 *Panorama* 가상 어플라이언스 *Panorama* 모드가 포함됩니다.

중복성을 활성화하면 더 많은 로그가 생성되기 때문에 이 구성에는 더 많은 저장 용량이 필요합니다. 중복을 활성화하면 수집기 그룹에서 로그 처리 트래픽이 두 배로 늘어나 최대 로깅 속도가 절반으로 줄어듭니다. 각 로그 수집기는 수신하는 각 로그의 복사본을 배포해야 하기 때문입니다. *(*컬렉터 그룹의 공간이 부족하면 오래된 로그를 삭제합니다.*)*

©2024 Palo Alto Networks, Inc.

Panorama HA 피어 간의 동기화

Panorama HA 피어는 활성 Panorama 피어에서 변경 사항을 커밋할 때마다 실행 중인 구성을 동기화합니다. 후보 구성은 활성 피어에 구성을 저장할 때마다 또는 페일오버가 발생하기 직전에 피어 간에 동기화됩니다.

공유 개체 및 정책 규칙, 디바이스 그룹 개체 및 규칙, 템플릿 구성, 인증서 및 SSL/TLS 서비스 프로파일, 관리 액세스 구성과 같이 쌍 간에 공통적인 설정은 Panorama HA 피어 간에 동기화됩니다.

자동 커밋 복구 활성화인 경우 HA 동기화는 Panorama에서 푸시한 후 방화벽이 자체와 Panorama 간의 연결을 성공적으로 테스트한 후에만 발생합니다.

동기화되지 않는 설정은 다음과 같이 각 피어에 고유한 설정입니다.

- Panorama HA 구성 - 우선 순위 설정, 피어 IP 주소, 경로 모니터링 그룹 및 IP 주소
- Panorama 구성 - 관리 인터페이스 IP 주소, FQDN 설정, 로그인 배너, NTP 서버, 시간대, 지리적 위치, DNS 서버, Panorama 액세스에 허용된 IP 주소, SNMP 시스템 설정 및 동적 콘텐츠 업데이트 일정
- 예약된 구성 내보내기
- 로깅을 위한 NFS 파티션 구성 및 모든 디스크 할당량 할당. 이는 VMware ESXi 서버에서 실행되는 레거시 모드의 Panorama 가상 어플라이언스에만 적용됩니다.
- Panorama 로컬 스토리지(SSD)의 다양한 유형의 로그 및 데이터베이스에 대한 디스크 한도 할당

  마스터 키를 사용하여 *Panorama*에서 개인 키와 인증서를 암호화하는 경우 두 *HA* 피어에서 동일한 마스터 키를 사용해야 합니다. 마스터 키가 다른 경우 *Panorama*는 *HA* 피어를 동기화할 수 없습니다.
- Panorama ###의 암호

자세한 내용은 Panorama HA 전제 조건 또는 Panorama에서 HA 설정을(를) 참조하십시오.

©2024 Palo Alto Networks, Inc.

Panorama HA 쌍 관리

- Panorama에서 HA 설정
- HA 피어 간에 사용자 지정 인증서를 사용하여 인증 설정
- Panorama HA 페일오버 테스트
- NFS 로깅을 재개하기 위해 Panorama 페일오버 후 우선 순위 전환
- 기본 Panorama를 활성 상태로 복원

소프트웨어 또는 콘텐츠 업데이트를 설치하려면 HA 구성에서 Panorama 업데이트 설치를 참조하십시오.

Panorama에서 HA 설정

다음 단계를 수행하기 전에 Panorama HA 전제 조건을(를) 검토합니다.

Panorama HA 피어 간에 통신 보안 설정을 구성하면 *Panorama HA* 피어가 서로 인증하도록 지정된 사용자 지정 인증서를 사용합니다. 그렇지 않으면 *Panorama HA* 피어가 사전 정의된 인증서를 인증에 사용합니다.

Panorama HA 피어가 통신을 인증하도록 구성하는 방법에 관계없이 *Panorama HA* 피어가 서로 통신하는 기능에는 영향을 미치지 않습니다.

STEP 1 | HA 피어에서 MGT 포트 간의 연결을 설정합니다.

Panorama 피어는 MGT 포트를 사용하여 서로 통신합니다. HA 쌍에서 Panorama 서버의 MGT 포트에 할당한 IP 주소가 라우팅 가능하고 피어가 네트워크를 통해 서로 통신할 수 있는지 확인하십시오. MGT 포트를 설정하려면 Panorama 가상 어플라이언스의 초기 구성 수행 또는 M-시리즈 어플라이언스의 초기 구성 수행을(를) 참조하십시오.

쌍에서 **Panorama** 피어를 선택한 다음 나머지 작업을 완료합니다.

STEP 2 | HA를 활성화하고 (선택 사항) HA 연결에 대한 암호화를 활성화합니다.

1. **Panorama** > 고가용성을 선택한 다음 설정 섹션을 편집합니다.
2. **HA** 활성화를 선택합니다.
3. 피어 **HA IP** 주소 필드에 피어 Panorama에 할당된 IP 주소를 입력합니다.
4. 피어 **HA** 일련번호 필드에 피어 Panorama의 일련번호를 입력합니다.

   Panorama HA 피어 일련 번호를 입력하면 Panorama IP에 대한 무차별 대입 공격에 대한 공격 표면이 줄어듭니다.
5. 모니터 보류 시간 필드에 시스템이 제어 링크 실패에 대해 조치를 취하기 전에 대기할 시간(밀리초)을 입력합니다(범위는 1000-60000, 기본값은 3000).
6. 암호화를 원하지 않는 경우 암호화 사용 체크박스의 선택을 취소하고 확인을 클릭합니다. 추가 단계는 필요하지 않습니다. 암호화를 원하는 경우 암호화 사용 체크박스를 선택한 다음 확인을 클릭한 후 다음 작업을 수행합니다.

   1. **Panorama** > 인증서 관리 > 인증서를 선택합니다.

©2024 Palo Alto Networks, Inc.

2. **HA** 키 내보내기를 선택합니다. 피어 Panorama가 액세스할 수 있는 네트워크 위치에 HA 키를 저장합니다.
3. 피어 **Panorama** > **Certificate Management** > **Certificates**로 이동하고 **HA** 키 가져오기를 선택한 다음 키를 저장한 위치로 이동하여 가져옵니다.

STEP 3 | HA 우선 순위를 설정합니다.

1. **Panorama** > 고가용성에서 일렉션**(Election)** 설정 섹션을 편집합니다.
2. 디바이스 우선 순위를 기본 또는 보조로 정의합니다. 한 피어를 기본으로 설정하고 다른 피어를 보조로 설정해야 합니다.

   두 피어의 우선 순위 설정이 같으면 일련번호가 더 높은 피어가 일시 중단된 상태가 됩니다.
3. 선점 동작을 정의합니다. 기본적으로 선점은 활성화되어 있습니다. 선점 선택(활성화 또는 비활성화)은 두 피어에서 동일해야 합니다.

   로깅에 *NFS*를 사용 중이고 선점을 비활성화한 경우 *NFS*에 대한 로깅을 재개하려면 NFS 로깅을 재개하기 위해 Panorama 페일오버 후 우선 순위 전환을(를) 참조하십시오.

STEP 4 | 경로 모니터링을 구성하려면 하나 이상의 경로 그룹을 정의하십시오.

경로 그룹에는 Panorama가 네트워크 연결을 확인하기 위해 핑(ping)해야 하는 대상 IP 주소(노드)가 나열됩니다.

모니터링할 노드가 포함된 각 경로 그룹에 대해 다음 단계를 수행하십시오.

1. **Panorama** > 고가용성을 선택한 다음 경로 그룹 섹션에서 추가를 클릭합니다.
2. 경로 그룹의 이름을 입력합니다.
3. 이 그룹에 대한 실패 조건을 선택합니다.
   - **any**는 IP 주소 중 하나에 연결할 수 없는 경우 경로 모니터링 실패를 트리거합니다.
   - **all**은 연결할 수 있는 IP 주소가 없는 경우에만 경로 모니터링 실패를 트리거합니다.
4. 모니터링하려는 각 대상 IP 주소를 추가합니다.
5. 확인을 클릭합니다. 경로 그룹 섹션에 새 그룹이 표시됩니다.

STEP 5 | (선택 사항) Panorama에서 경로 모니터링을 위한 실패 조건을 선택합니다.

1. **Panorama** > 고가용성을 선택한 다음 경로 모니터링 섹션을 편집합니다.
2. 실패 조건 선택:
   - **all**은 모니터링되는 모든 경로 그룹이 실패하는 경우에만 페일오버를 트리거합니다.
   - **any**는 모니터링되는 경로 그룹이 실패할 때 페일오버를 트리거합니다.
3. 확인을 클릭합니다.

STEP 6 | 구성 변경 사항을 커밋합니다.

커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 다른 Panorama 피어를 구성합니다.

HA 쌍의 다른 피어에서 2단계~6단계를 반복합니다.

STEP 8 | Panorama 피어를 동기화합니다.

1. 활성 Panorama에서 대시보드에 액세스하고 위젯 > 시스템 > 고가용성을 선택하여 HA 위젯을 표시합니다.
2. 피어에 동기화하고 예를 클릭한 다음 실행 중인 구성이 동기화됨을 표시할 때까지 기다립니다.
3. 패시브 Panorama에서 대시보드에 액세스하고 위젯 > 시스템 > 고가용성을 선택하여 HA 위젯을 표시합니다.
4. 실행 중인 구성이 동기화됨을 표시하는지 확인합니다.

STEP 9 | (선택 사항) HA 피어 간에 사용자 지정 인증서를 사용하여 인증 설정.

두 Panorama HA 피어 모두에 대해 통신 보안 설정을 구성해야 합니다. HA 구성에서 Panorama에 대한 통신 보안 설정을 구성해도 HA 피어 간의 HA 연결에는 영향을 미치지 않습니다. 그러나 통신 보안 설정이 잘못 구성되었거나 HA 피어 또는 관리 방화벽에 올바른 인증서가 없거나 인증서가 만료된 경우 통신 보안 링크를 통과하는 기능이 실패할 수 있습니다.

통신 보안 설정을 구성하여 설정된 링크의 모든 트래픽은 항상 암호화됩니다.

HA 구성에서 *Panorama*에 대한 통신 보안 설정을 구성하는 경우 보안 서버 통신도 사용자 정의가 요구됩니다. 그렇지 않으면 관리 방화벽 및 *WildFire* 어플라이언스가 *Panorama*에 연결될 수 없고 *PAN-OS* 기능이 영향을 받습니다.

HA 피어 간에 사용자 지정 인증서를 사용하여 인증 설정

Panorama HA 피어 간의 HA 연결을 보호하기 위해 사용자 지정 인증서를 사용하여 인증을 설정할 수 있습니다.

STEP 1 | Panorama에서 인증 기관(CA) 인증서를 생성합니다.

1. **Panorama** > 인증서 관리 > 인증서를 선택합니다.
2. 자체 서명된 루트 CA 인증서를 생성하거나 엔터프라이즈 CA에서 인증서를 가져옵니다.

STEP 2 | 루트 CA 및 중간 CA를 포함하는 인증서 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > 인증서 프로파일을 선택합니다.
2. 인증서 프로파일을 구성합니다.

STEP 3 | SSL/TLS 서비스 프로파일을 구성합니다.

1. **Panorama** > 인증서 관리 > **SSL/TLS** 서비스 프로파일을 선택합니다.
2. Panorama 및 해당 관리형 디바이스가 SSL/TLS 서비스에 사용하는 인증서 및 프로토콜을 정의하도록 SSL/TLS 프로파일을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 기본 HA 피어의 Panorama에서 통신 보안 설정을 구성합니다.

HA 구성에서 *Panorama - Panorama*의 통신 보안 설정을 구성하는 경우 보안 서버 통신도 사용자 정의해야 합니다. 그렇지 않으면 관리 방화벽, 전용 로그 수집기 및 *WildFire* 어플라이언스는 *Panorama*에 연결할 수 없고 *PAN-OS* 기능이 영향을 받습니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 통신 보안 설정을 편집합니다.
2. 인증서 유형으로 로컬을 선택합니다.
3. 이전 단계에서 구성한 인증서 및 인증서 프로파일을 선택합니다.
4. **HA Communication**, **WildFire Communication** 및 데이터 재배포를 확인(활성화)합니다.
5. 보안 서버 통신 사용자 지정을 선택(활성화)합니다.
6. SSL/TLS 서비스 프로파일 드롭다운에서 **SSL/TLS** 서비스 프로파일을 선택합니다. 이 SSL/TLS 서비스 프로파일은 Panorama, 방화벽, 로그 수집기 및 Panorama의 HA 피어 간의 모든 SSL 연결에 적용됩니다.
7. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
8. 권한 부여 목록을 구성합니다.

   HA 구성에서 *Panorama*에 대한 통신 보안 설정을 구성할 때 *Panorama HA* 피어를 인증 목록에 추가해야 합니다.

   1. 인증 목록에서 추가를 클릭합니다.
   2. 주체 또는 주체 대체 이름을 식별자 유형으로 선택합니다.
   3. 일반 이름 입력
9. (선택 사항) 사용자 지정 인증서만 허용 체크박스가 선택되어 있지 않은지 확인합니다. 이를 통해 사용자 지정 인증서로 마이그레이션하는 동안 모든 디바이스를 계속 관리할 수 있습니다.

   사용자 지정 인증서만 허용 체크박스가 선택된 경우 *Panorama*는 사전 정의된 인증서를 사용하여 디바이스를 인증하지 않고 관리할 수 없습니다.
10. 연결 끊기 대기 시간(분)에 Panorama가 관리 디바이스와의 연결을 끊고 다시 설정하기 전에 기다려야 하는 시간(분)을 입력합니다. 이 필드는 기본적으로 비어 있으며 범위는 0~44,640분입니다.

    연결 해제 대기 시간은 새 구성을 커밋할 때까지 카운트다운을 시작하지 않습니다.

1. 확인을 클릭합니다.
2. 커밋 및 **Panorama**에 커밋.
3. 보조 Panorama HA 피어에서 이 단계를 반복합니다.

   보조 Panorama HA 피어에서 통신 보안 설정을 구성할 때 위에서 설명한 대로 기본 HA 피어를 인증 목록에 추가합니다.

STEP 5 | 클라이언트 측 Panorama를 PAN-OS 10.1로 업그레이드하십시오.

Panorama를 업그레이드하십시오.

 ©2024 Palo Alto Networks, Inc.

Panorama HA 페일오버 테스트

HA 구성이 제대로 작동하는지 테스트하려면 수동 페일오버를 트리거하고 피어 전환 상태가 성공적인 상태인지 확인하십시오.

STEP 1 | 활성 Panorama 피어에 로그인합니다.

웹 인터페이스의 오른쪽 하단 모서리에서 Panorama 서버의 상태를 확인할 수 있습니다.

STEP 2 | 활성 Panorama 피어를 일시 중단합니다.

Panorama > **High Availability**를 선택한 다음 Operational Commands 섹션에서 **Suspend local Panorama** 링크를 클릭합니다.

STEP 3 | 수동 Panorama 피어가 활성으로 인계되었는지 확인합니다.

Panorama 대시보드, 고가용성 위젯에서 로컬 수동 서버의 상태가 활성이고 피어의 상태가 일시 중단되었는지 확인합니다.

STEP 4 | 일시 중단된 피어를 기능 상태로 복원합니다. 몇 분 동안 기다린 다음 선점이 활성화된 경우 선점이 발생했는지 확인합니다.

이전에 일시 중단한 Panorama에서 다음을 따릅니다.

1. **Panorama** > 고가용성을 선택한 다음 작동 명령 섹션에서 로컬 **Panorama**로 설정 작동을 클릭합니다.
2. 대시보드의 고가용성 위젯에서 이 (로컬) Panorama가 활성 피어로 인계되었고 다른 피어가 이제 수동 상태인지 확인합니다.

NFS 로깅을 재개하기 위해 Panorama 페일오버 후 우선 순위 전환

ESXi 서버에서 실행되는 레거시 모드의 Panorama 가상 어플라이언스는 로깅을 위해 NFS 데이터 저장소를 사용할 수 있습니다. HA 구성에서는 기본 Panorama 피어만 NFS 기반 로그 파티션에 마운트되고 NFS에 쓸 수 있습니다. 페일오버가 발생하고 수동 Panorama가 활성 상태가 되면 활성-보조 상태가 됩니다. 보조 Panorama 피어는 방화벽을 능동적으로 관리할 수 있지만 NFS 파티션을 소유하지 않기 때문에 로그를 수신하거나 NFS에 쓸 수 없습니다. 방화벽이 기본 Panorama 피어로 로그를 포워딩할 수 없는 경우 각 방화벽은 로그를 로컬 디스크에 씁니다. 방화벽은 수동-기본 Panorama를 다시 사용할 수 있게 되면 다시 Panorama로 로그를 포워딩할 수 있도록 Panorama에 포워딩한 마지막 로그 항목 집합에 대한 포인터를 유지합니다.

이 섹션의 지침을 사용하여 활성-보조 Panorama 피어가 NFS 파티션에 대한 로깅을 시작할 수 있도록 우선 순위를 수동으로 전환합니다. 이 변경을 트리거해야 하는 일반적인 시나리오는 다음과 같습니다.

- 선점이 비활성화되었습니다. 기본적으로 Panorama에서는 선점이 활성화되고 기본 피어가 다시 사용 가능해지면 활성 상태로 재개됩니다. 선점이 비활성화되면 보조 피어의 우선 순위를 기본 피어로 전환하여 NFS 파티션을 마운트하고 관리 방화벽에서 로그를 수신하고 NFS 파티션에 쓸 수 있도록 해야 합니다.
- 활성 Panorama는 실패하고 단기간에 실패에서 복구할 수 없습니다. 우선 순위를 전환하지 않으면 방화벽의 최대 로그 저장 용량에 도달하면 가장 오래된 로그를 덮어써서 로컬 디스크에 계속 로깅할 수 있습니다. 이 상황에서는 로그가 손실될 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 현재 수동-기본 Panorama에 로그인하고 **Panorama** > 설정 > 작업을 선택한 다음 디바이스 작업 섹션에서 **Panorama** 중지를 클릭합니다.

STEP 2 | 활성-보조 Panorama에 로그인하고 **Panorama** > 고가용성을 선택한 다음 일렉션(Election) 설정을 편집하고 우선 순위를 기본으로 설정합니다.

STEP 3 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 4 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

메시지가 표시되면 재부팅하지 마십시오.

STEP 5 | Panorama CLI에 로그인하고 다음 명령을 입력하여 NFS 파티션의 소유권을 **`request high-availability convert-to-primary`** 피어로 변경합니다.

STEP 6 | **Panorama** > 설정 > 작업을 선택한 다음 디바이스 작업 섹션에서 **Panorama** 재설정을 클릭합니다.

STEP 7 | 1단계에서 전원을 끈 Panorama 피어의 전원을 켭니다. 이 피어는 이제 수동 보조 상태가 됩니다.

기본 Panorama를 활성 상태로 복원

기본적으로 Panorama의 선점 기능을 사용하면 기본 Panorama가 사용 가능한 즉시 활성 피어로 기능을 재개할 수 있습니다. 그러나 선점이 비활성화된 경우 장애, 작동하지 않거나 일시 중단된 상태에서 복구한 후 기본 Panorama를 강제로 활성화하는 유일한 방법은 보조 Panorama 피어를 일시 중단하는 것입니다.

활성-보조 Panorama는 일시 중단된 상태가 되기 전에 커밋되지 않은 모든 구성 변경 사항이 저장되고 다른 피어에서 액세스할 수 있도록 후보 구성을 수동 Panorama로 전송합니다.

STEP 1 | Panorama를 일시 중단합니다.

1. 일시 중단 상태에 두려는 Panorama 피어에 로그인합니다.
2. **Panorama** > 고가용성을 선택한 다음 작동 명령 섹션에서 로컬 **Panorama** 일시 중단 링크를 클릭합니다.

STEP 2 | 상태가 사용자 요청에 따라 Panorama가 일시 중단되었음을 나타내는지 확인합니다.

대시보드의 고가용성 위젯에서 로컬 상태가 일시 중단되었는지 확인합니다.

피어를 일시 중단하면 페일오버가 트리거되고 다른 Panorama가 활성 피어로 인계됩니다.

STEP 3 | 일시 중단된 Panorama를 기능 상태로 복원합니다.

1. **Panorama** > 고가용성 탭의 작동 명령 섹션에서 로컬 **Panorama**가 작동하도록 설정 기능 링크를 클릭합니다.
2. 대시보드의 고가용성위젯에서 Panorama가 활성 또는 수동 상태로 전환되었는지 확인합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 관리

이 섹션에서는 Panorama™ 관리 서버를 관리하고 유지 관리하는 방법을 설명합니다. 여기에는 다음 주제가 포함됩니다.

- 구성 변경 사항 미리보기, 검증 또는 커밋
- 관리되는 디바이스에 대한 선택적 구성 변경 커밋
- 선택적 구성 변경 내용을 관리형 디바이스에 푸시
- 자동 커밋 복구 활성화
- Panorama 및 방화벽 구성 백업 관리
- Panorama 구성의 변경 사항 비교
- 구성 변경 제한을 위한 잠금 관리
- Panorama에 사용자 정의 로고 추가
- Panorama 작업 관리자 사용
- 로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 관리
- 모니터 Panorama
- Panorama 재부팅 또는 종료
- Panorama 암호 프로파일 및 복잡성 구성

네트워크 액세스 설정 정의, 라이선스 부여, Panorama 소프트웨어 버전 업그레이드 및 Panorama에 대한 관리 액세스 설정을 포함한 초기 설정 완료에 대한 지침은 Panorama 설정을(를) 참조하십시오.

구성 변경 사항 미리보기, 검증 또는 커밋

Panorama 구성에 대해 보류 중인 변경 사항에 대해 Panorama 커밋, 검증 및 미리보기 작업을(를) 수행한 다음 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터를 포함하여 Panorama가 관리하는 어플라이언스에 이러한 변경 사항을 푸시할 수 있습니다. 관리자 또는 위치별로 보류 중인 변경 사항을 필터링한 다음 해당 변경 사항만 커밋, 푸시, 유효성 검사 또는 미리 볼 수 있습니다. 위치는 특정 디바이스 그룹, 템플릿, 수집기 그룹, 로그 수집기, 공유 설정 또는 Panorama 관리 서버일 수 있습니다.

Panorama는 실행 중인 구성을 푸시하기 때문에 Panorama에 처음 커밋할 때까지 변경 사항을 디바이스에 푸시할 수 없습니다. 변경 사항을 디바이스에서 활성화할 준비가 되지 않은 경우 커밋 > **Panorama**에 커밋을 선택하여 변경 사항을 디바이스에 푸시하지 않고 Panorama 구성에 커밋할 수 있습니다. 나중에 디바이스에서 변경 사항을 활성화할 준비가 되면 커밋 > 디바이스에 푸시를 선택할 수 있습니다. Panorama와 디바이스 모두에서 변경 사항을 활성화할 준비가 되면 다음 절차에 설명된 대로 커밋 > 커밋 및 푸시를 선택합니다.

(디바이스 그룹만 해당) 상위 디바이스 그룹에 대한 구성을 변경할 때 이러한 변경 사항을 하위 디바이스 그룹과 연결된 관리형 방화벽에 푸시하는 기능은 Panorama 웹 인터페이스에서만 지원됩니다. 이 경우 Panorama CLI에서 푸시된 디바이스 그룹 구성 변경은 영향을 받는 디바이스 그룹과 직접 연결된 관리형 방화벽에만 푸시되며 하위 디바이스 그룹과 연결된 관리형 방화벽에는 푸시되지 않습니다. 하위 디바이스 그룹은 *Panorama* 웹 인터페이스에서 상위 디바이스 그룹에 대한 디바이스 그룹 구성 변경을 푸시할 때 기본적으로 선택되며 *Panorama CLI*에서 푸시할 때는 기본적으로 포함되지 않습니다.

예를 들어, 두 개의 방화벽이 연결된 *ParentDG1*과 서로 다른 두 개의 관리형 방화벽이 연결된 *ChildDG2*를 생성한다고 가정해 보겠습니다. *ParentDG1*의 구성을 변경합니다.

이 시나리오에서는 *Panorama* 웹 인터페이스에서 디바이스로 푸시하고 커밋 및 푸시를 실행하면*ParentDG1* 변경 사항이 *4*개의 방화벽 모두에 성공적으로 푸시됩니다. 그러나 *Panorama CLI*의 ***commit-all*** 작업은 *ParentDG1*과 연결된 관리형 방화벽으로만 푸시됩니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 커밋, 유효성 검사 또는 미리 볼 구성 변경 범위를 구성합니다.

1. 웹 인터페이스 상단에서 커밋을 클릭합니다.
2. 다음 옵션 중 하나를 선택합니다.
   - 모든 변경 사항 커밋(기본값) - 관리 권한이 있는 모든 변경 사항에 커밋을 적용합니다. 이 옵션을 선택하면 커밋 범위를 수동으로 필터링할 수 없습니다. 대신 로그인에 사용한 계정에 할당된 관리자 역할에 따라 커밋 범위가 결정됩니다.
   - 커밋 변경 작성자 - 관리자 또는 위치별로 커밋 범위를 필터링할 수 있습니다. 로그인에 사용한 계정에 할당된 관리 역할에 따라 필터링할 수 있는 변경 사항이 결정됩니다.

   다른 관리자의 변경 사항을 커밋하려면 로그인에 사용한 계정에 운용 관리자 역할 또는 다른 관리자를 위한 커밋 권한이 활성화된 관리자 역할 프로파일이 할당되어야 합니다.
3. (선택 사항) 커밋 범위를 관리자별로 필터링하려면 커밋 변경자를 선택한 다음 인접한 링크를 클릭한 다음 관리자를 선택한 다음 확인을 클릭합니다.
4. (선택 사항) 위치별로 필터링하려면 커밋 변경자를 선택한 다음 커밋 범위에서 제외할 변경 사항을 선택 취소합니다.

   포함 및 제외된 구성 변경 간의 종속성으로 인해 유효성 검사 오류가 발생하면 모든 변경 사항을 포함하여 커밋을 수행합니다. 예를 들어, 디바이스 그룹에 대한 변경 사항을 커밋할 때 해당 디바이스 그룹의 동일한 규칙 베이스에 대한 규칙을 추가, 삭제 또는 재배치한 모든 관리자의 변경 사항을 포함해야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 커밋이 활성화할 변경 사항을 미리 봅니다.

동일한 디바이스를 삭제한 후 정책 규칙에 다시 추가한 후 변경 사항을 미리 보면 *Panorama*는 동일한 디바이스를 실행 중인 구성에서 삭제된 것과 후보 구성에서 모두 추가한 것으로 표시합니다. 또한 실행 중인 구성의 디바이스 대상 목록에 있는 디바이스의 순서는 후보 구성과 다를 수 있으며 구성 변경 사항이 없는 경우에도 변경 사항을 미리 볼 때 변경 사항으로 표시됩니다.

예를 들어 모든 변경 사항이 기억나지 않고 모든 변경 사항을 활성화하고 싶지 않은 경우에 유용할 수 있습니다.

Panorama는 커밋 범위에서 선택한 구성을 실행 중인 구성과 비교합니다. 미리보기 창은 구성을 나란히 표시하고 색상 코딩을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색)에 해당하는 변경 사항을 나타냅니다.

변경 사항을 미리 보고 강조 표시된 차이점 전후에 표시할 비교 구성 파일의 줄 수인 컨텍스트 줄을 선택합니다. 이 라인은 미리보기 출력을 웹 인터페이스의 설정과 연관시키는 데 도움이 됩니다. 변경 사항 검토가 끝나면 미리보기 창을 닫습니다.

*Panorama*를 *PAN-OS 10.1* 이상 릴리즈로 업그레이드한 후 변경 사항 미리 보기에 *##-hip-any* 및 *##-hip-any*라는 *HIP* 프로파일이 *hip-profiles-any* 대신 *PAN-OS 9.1* 이전 릴리즈를 실행하는 모든 관리 방화벽의 각 보안 정책 규칙에 추가되었음을 보여줍니다. 이는 *Panorama*가 *PAN-OS 10.0* 이상 릴리스에서 실행 중인 구성과 후보 구성을 비교하는 데 사용하는 *XML* 파일이 변경되었기 때문입니다. 푸시가 성공하므로 이 오류를 무시해도 됩니다.

미리보기 결과가 새 창에 표시되기 때문에 브라우저에서 팝업 창을 허용해야 합니다. 미리보기 창이 열리지 않으면 브라우저 설명서에서 팝업 창 차단을 해제하는 단계를 참조합니다.

STEP 3 | 변경 사항을 커밋할 개별 설정을 미리 봅니다.

이는 설정 유형 및 변경한 사람과 같은 변경 사항에 대한 세부 정보를 알고자 할 때 유용할 수 있습니다.

1. 변경 요약을 클릭합니다.
2. (선택 사항) 열 이름별로 그룹화(예: 설정 유형).
3. 변경 사항 검토를 마치면 변경 사항 요약 대화 상자를 닫습니다.

STEP 4 | 커밋이 성공할 수 있도록 커밋하기 전에 변경 사항을 확인하십시오.

1. 변경 사항을 확인합니다.

   결과에는 실제 커밋이 표시할 모든 오류와 경고가 표시됩니다.
2. 유효성 검사 결과가 식별하는 모든 오류를 해결합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | (선택 사항) 푸시 범위를 수정합니다.

기본적으로 푸시 범위에는 Panorama 커밋이 필요한 변경 사항이 있는 모든 위치가 포함됩니다.

커밋 > 디바이스에 푸시를 선택하면 푸시 범위에는 *Panorama* 실행 구성과 동기화되지 않은 디바이스와 연결된 모든 위치가 포함됩니다.

1. 특정 디바이스를 수동으로 선택하려면 기본 선택 사항이 없습니다. Panorama가 푸시하는 기본 디바이스는 영향을 받는 디바이스 그룹 및 템플릿 구성 변경 사항을 기반으로 합니다.
2. 선택 사항을 편집하여 푸시 범위를 수정합니다.
   - 디바이스 그룹 - 디바이스 그룹 또는 개별 방화벽 또는 가상 시스템을 선택합니다.
   - 템플릿 - 템플릿, 템플릿 스택(template stack) 또는 개별 방화벽을 선택합니다.
   - 수집기 그룹 - 수집기 그룹을 선택합니다.
   - 디바이스 후보 구성과 병합 — 이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 Panorama의 구성 푸시와 병합합니다. 로컬 방화벽 구성은 Panorama에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 로컬 방화벽 구성이 병합되고 커밋됩니다.

     Panorama 관리 구성과 별도로 로컬 방화벽 구성 변경을 관리하고 커밋하는 경우 이 설정을 비활성화합니다.
3. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.

STEP 6 | 디바이스 그룹 또는 템플릿에 푸시할 변경 사항을 확인합니다.

1. 디바이스 그룹 푸시를 검증하거나 템플릿 푸시를 검증합니다.

   결과에는 실제 푸시 작업이 표시할 모든 오류 및 경고가 표시됩니다.
2. 유효성 검사 결과가 식별하는 모든 오류를 해결합니다.

STEP 7 | Panorama에 변경 사항을 커밋하고 변경 사항을 디바이스에 푸시합니다.

구성 변경 사항을 커밋하고 푸시합니다.

Panorama 작업 관리자 사용 보류 중이거나(선택적으로 취소할 수 있음), 진행 중이거나 완료되었거나 실패한 커밋에 대한 세부 정보를 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 8 | Panorama에서 구성이 성공적으로 푸시되었는지 확인합니다.

1. 방화벽 CLI에 로그인합니다.
2. 다음 명령 중 하나를 실행합니다.

```
admin> show config pushed-template
```

```
admin> show config merged
```

특정 구성 개체에 대한 `show` 명령은 Panorama 푸시된 구성이 아니라 로컬 방화벽 구성만 표시하도록 설계되었습니다.

예를 들어, 방화벽 CLI에서 실행된 `show network virtual router` 명령은 방화벽에 있는 가상 라우터 구성만 표시하고 Panorama 푸시된 가상 라우터 구성은 표시하지 않습니다.

©2024 Palo Alto Networks, Inc.

관리되는 디바이스에 대한 선택적 구성 변경 커밋

Panorama™ 관리 서버에서 구성 변경은 자주 발생하며 일반적으로 Panorama에서 수행된 다른 구성 변경 사항을 알지 못하는 여러 관리자가 수행합니다. Panorama에 커밋할 구성 개체를 제어하고 불완전한 구성이 Panorama에서 관리 방화벽으로 푸시되는 것을 방지할 수 있는 것이 중요합니다. 보류 중인 모든 구성 변경 사항을 Panorama에 커밋하는 대신 커밋할 특정 디바이스 그룹 및 템플릿 스택 개체를 선택할 수 있습니다. 선택적 커밋이 성공하면 시스템 로그가 생성됩니다.

커밋할 특정 개체를 선택하는 기능을 사용하면 커밋할 준비가 되지 않은 구성 변경을 수행하는 다른 관리자를 방해하지 않고 여러 관리자가 구성 변경을 효과적으로 수행할 수 있습니다. Panorama에 구성 변경 사항을 선택적으로 커밋하는 기능을 활용하면 정의된 운영 절차를 유지하면서 운영 범위 내에서 정의되지 않은 독립적인 구성 변경을 성공적으로 수행할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | Panorama에서 디바이스 그룹 및 템플릿 스택 구성 변경을 수행합니다.

STEP 3 | 커밋 및 **Panorama**에 커밋.

STEP 4 | 커밋 범위를 **Commit Changes Made By**로 변경하여 Panorama에 커밋할 특정 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택합니다.

푸시 범위에는 현재 로그인한 관리자의 이름이 표시됩니다. 관리자 이름을 클릭하면 Panorama에 커밋되지 않은 구성 변경을 수행한 관리자 목록을 볼 수 있습니다.

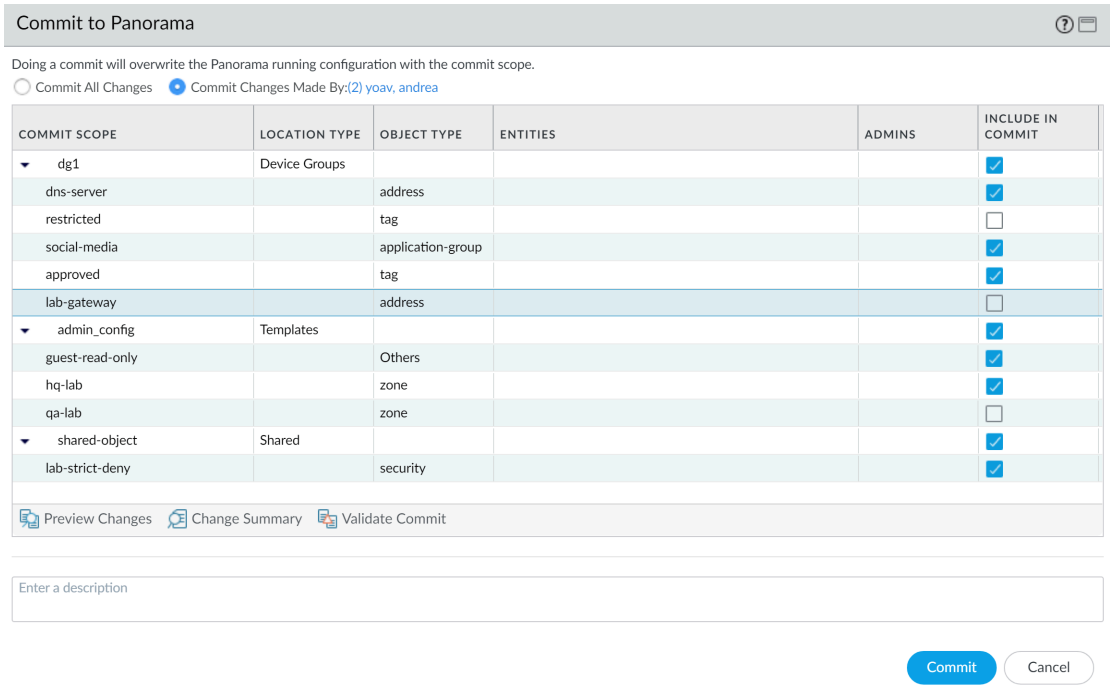
STEP 5 | Include in Commit 열에서 커밋에 포함할 구성 개체를 선택(활성화)합니다.

STEP 6 | (선택 사항) 보류 중인 구성 변경 사항을 미리 보고 유효성을 검사하여 선택적인 구성 변경 사항을 Panorama에 커밋할 것인지 확인합니다.

©2024 Palo Alto Networks, Inc.

STEP 7 | 커밋합니다.

커밋 상태 페이지는 커밋된 구성 변경을 수행한 관리자와 커밋된 구성 변경 위치를 표시합니다.



STEP 8 | 선택적 구성 변경 내용을 관리형 디바이스에 푸시.

선택한 구성 개체를 Panorama에 커밋한 후 해당 구성 개체를 관리형 방화벽으로 푸시할 수 있습니다.

©2024 Palo Alto Networks, Inc.

선택적 구성 변경 내용을 관리형 디바이스에 푸시

하나 이상의 Panorama 관리자가 관리형 방화벽으로 푸시하기 위해 커밋한 구성 변경 사항을 포함할 수 있습니다. 이렇게 하면 구성을 변경할 때 더 높은 수준의 제어가 가능하며 불완전한 구성을 관리형 방화벽으로 푸시할 위험이 줄어듭니다. Panorama 관리자가 구성 변경 내용을 선택적으로 푸시할 수 있도록 하려면 선택적 푸시를 허용하는 관리자 역할 프로파일을 구성하고 Panorama 관리자에게 관리자 역할 프로파일을 할당해야 합니다. 관리형 방화벽에 대한 성공적인 선택적 푸시를 위해 시스템 로그가 생성됩니다.

또한 구성 변경 내용을 관리형 방화벽에 푸시할 때 추가 선택성을 위해 구성 변경의 선택적 커밋을 활용할 수도 있습니다. 선택적 커밋을 사용하면 특정 구성 개체를 선택하고 커밋할 수 있습니다. 커밋한 후 선택적 푸시를 활용하여 다른 *Panorama* 관리자가 수행한 모든 커밋된 구성 변경 사항을 검토하고 푸시할 수 있습니다.

관리형 방화벽에 대한 푸시에 포함할 Panorama 관리자 구성 변경 사항을 지정하는 기능을 사용하면 여러 관리자가 다른 관리자를 방해하지 않고 방화벽 구성을 효과적으로 관리할 수 있으며 불완전한 구성을 관리형 방화벽으로 푸시하여 중단될 수 있는 위험을 줄일 수 있습니다. 구성 변경을 선택적으로 푸시하는 기능을 활용하면 정의된 운영 절차를 유지하면서 작업 범위 내에 정의되지 않은 독립적인 구성 변경을 성공적으로 수행할 수 있습니다.

선택적 푸시는 관리형 방화벽에만 지원되며 지원되는 모든 PAN-OS 릴리스를 실행하는 관리형 방화벽에 대해 지원됩니다. 로그 수집기, 수집기 그룹, WildFire 어플라이언스 및 WildFire 클러스터에 대해서는 선택적 푸시가 지원되지 않습니다. 활성/수동 고가용성(HA) 구성의 Panorama의 경우 선택적 푸시는 활성 HA 피어에서만 지원됩니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

Panorama 관리자는 다른 관리자가 수행한 구성 변경 내용을 관리형 방화벽에 푸시할 수 있는 관리자 역할 프로파일로 구성해야 합니다. 기본 수퍼유저 또는 *Panorama* 관리자 역할 권한은 전체 개체 수준 구성 권한을 지원합니다.

STEP 2 | 커밋 및 디바이스에 푸시를 선택합니다.

커밋 및 푸시를 선택하여 선택적 구성 변경 사항을 Panorama에 커밋하고 이미 커밋된 변경 사항을 한 작업으로 푸시할 수도 있습니다.

커밋되지 않은 구성 변경은 선택적으로 푸시할 수 없습니다.

STEP 3 | 푸시 범위를 푸시 변경자로 변경하고 Panorama 관리자가 푸시 범위를 필터링하여 특정 디바이스 그룹 및 템플릿 스택 구성 변경 사항을 선택하여 관리형 방화벽에 푸시합니다.

푸시 범위에는 현재 로그인한 관리자의 이름이 표시됩니다. 관리자 이름을 클릭하여 관리형 방화벽에 푸시되지 않은 커밋된 구성 변경 사항이 있는 관리자 목록을 봅니다. 푸시 범위가 자동으로 새로 고쳐져 선택한 관리자를 기반으로 디바이스 그룹 및 템플릿 스택의 업데이트된 목록이 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 푸시에 포함 열에서 커밋에 포함할 구성 개체를 확인(사용)합니다.

푸시 범위에는 ##### ## 디바이스 그룹 및 템플릿 스택만 표시됩니다.

커밋된 전체 디바이스 그룹 또는 템플릿 스택 구성을 선택하고 푸시해야 합니다. 푸시 범위에 표시되는 개체 수준 변경 내용은 정보 제공용이며 선택한 디바이스 그룹 또는 템플릿 스택에 대한 푸시에서 제외할 수 없습니다.

STEP 5 | (선택 사항) 선택 항목을 편집하고 영향을 받는 디바이스 그룹 및 템플릿 스택과 연결된 관리형 방화벽을 선택합니다.

이 단계를 건너뛰면 영향을 받는 디바이스 그룹 및 템플릿 스택과 연결된 모든 관리형 방화벽으로 푸시합니다.

Panorama 관리 구성과 별도로 로컬 방화벽 구성 변경 사항을 관리하고 커밋하는 경우 디바이스 후보 구성과 병합 설정을 비활성화합니다.

이 설정은 기본적으로 활성화되어 있으며 보류 중인 모든 로컬 방화벽 구성을 *Panorama*의 구성 푸시와 병합합니다. 로컬 방화벽 구성은 *Panorama*에서 변경 사항을 푸시하는 관리자나 로컬 방화벽 구성을 변경한 관리자에 관계없이 로컬 방화벽 구성이 병합되고 커밋됩니다.

STEP 6 | 구성 변경 사항을 푸시합니다.

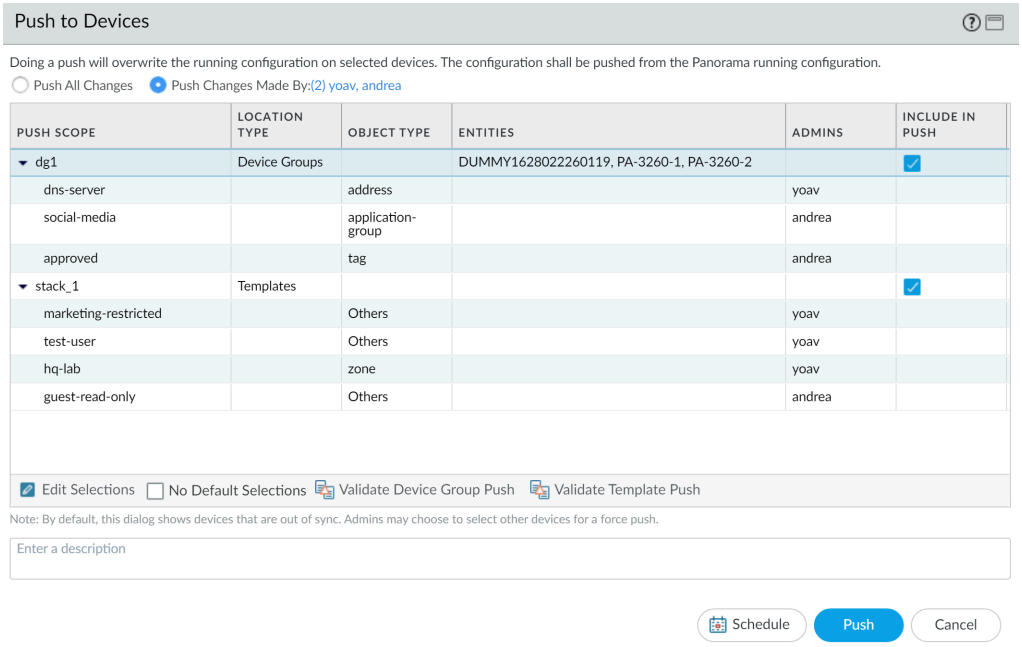
STEP 7 | 관리자 역할에서 다른 Panorama 관리자의 구성 변경 내용을 푸시할 수 있는 경우 디바이스에 푸시 확인 프롬프트 및 푸시를 검토합니다.

이 경고는 관리 범위에 포함된 관리자가 동일한 개체에 대해 구성을 충돌하여 변경할 때 표시됩니다. 예를 들어 Admin1은 구성 변경 내용을 관리형 방화벽으로 푸시할 수 있지만 Admin2는 허용되지 않습니다. Admin1은 `SecurityRule`을 만들고 ZoneA를 소스 영역으로 추가하며 변경 사항을 커밋합니다. 그런 다음 Admin2는 `SecurityRule`을 수정하고 ZoneA를 삭제하며 ZoneB를 추가하고 추가 구성을 변경합니다. Admin2는 Panorama에 변경 사항을 커밋합니다. Admin1은 관리형 방화벽으로의 푸

©2024 Palo Alto Networks, Inc.

시에 Admin1의 구성 변경 사항을 포함하려고 합니다. 이 시나리오에서는 `SecurityRule` 충돌에 대한 구성 변경 때문에 Admin1 푸시를 확인하라는 메시지가 표시됩니다.

다른 *Panorama* 관리자가 수행한 구성 변경 내용을 잘 모르는 경우 선택한 변경 내용만 계속 푸시하여 사용자 고유의 구성 변경 내용을 푸시하고 구성 개체가 변경한 내용과 충돌하는 내용을 덮어씁니다.



STEP 8 | **Panorama** > 관리형 디바이스 > 요약을 선택하고 영향을 받는 방화벽에 대한 템플릿 마지막 커밋 상태를 클릭하여 마지막 푸시 상태 세부 정보를 검토합니다.

©2024 Palo Alto Networks, Inc.

자동 커밋 복구 활성화

Panorama™ 관리 서버에서 관리되는 방화벽으로 푸시되거나 방화벽에서 로컬로 커밋된 구성 변경으로 인해 구성이 손상되었는지 확인하려면 자동 커밋 복구를 활성화하여 관리되는 방화벽이 각 커밋에 대한 구성 변경을 테스트하고 변경 사항이 변경되지 않았는지 확인합니다. Panorama와 관리 방화벽 간의 연결을 끊습니다. 각 관리 방화벽이 수행하는 테스트 수와 관리 방화벽이 실행 중인 이전 구성으로 구성을 자동으로 되돌리기 전에 각 테스트가 수행되는 간격을 구성할 수 있습니다. 자동 커밋 복구를 활성화하면 Panorama 구성이 아니라 관리형 방화벽 구성이 되돌려집니다. 또한 관리형 방화벽은 60분마다 Panorama에 대한 연결을 테스트하여 관련 없는 네트워크 구성이 변경되어 방화벽과 Panorama 간의 연결이 중단되거나 과거에 커밋된 구성의 영향이 연결에 영향을 미치는 경우 지속적인 통신을 보장합니다. 고가용성(HA) 구성의 경우 Panorama에서 푸시한 후 HA 피어 간의 HA 동기화는 연결 테스트 후에만 발생합니다.

자동 커밋 복구는 기본적으로 활성화되어 있습니다. 그러나 자동 커밋 복구를 비활성화한 다음 기존 프로덕션 환경에서 이 기능을 다시 활성화하려면 먼저 Panorama와 관리 방화벽 간의 연결을 끊는 정책 규칙이 없는지 확인하십시오. 예를 들어 관리 트래픽이 데이터플레인을 통과하는 경우 방화벽에서 Panorama로의 트래픽을 제한하는 정책 규칙이 있을 수 있습니다.

방화벽 구성이 마지막 실행 구성으로 성공적으로 되돌아간 후 방화벽은 구성 로그를 생성합니다. 또한 방화벽은 관리자가 이 기능을 비활성화할 때, 구성 푸시 후 실패한 연결 테스트로 인해 구성 되돌리기 이벤트가 시작될 때, 60분마다 수행되는 Panorama 연결 테스트가 실패하여 방화벽 구성을 되돌릴 때 시스템 로그를 생성합니다.



다른 구성 변경과 관계없이 자동 커밋 복구를 활성화합니다. *Panorama*와 관리 방화벽 간의 연결이 끊어지는 다른 구성 변경 사항과 함께 활성화된 경우 방화벽 구성을 자동으로 되돌릴 수 없습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 디바이스 > 설정 > 관리를 선택한 다음 템플릿 컨텍스트 드롭다운에서 원하는 템플릿 또는 템플릿 스택을 선택합니다.

©2024 Palo Alto Networks, Inc.

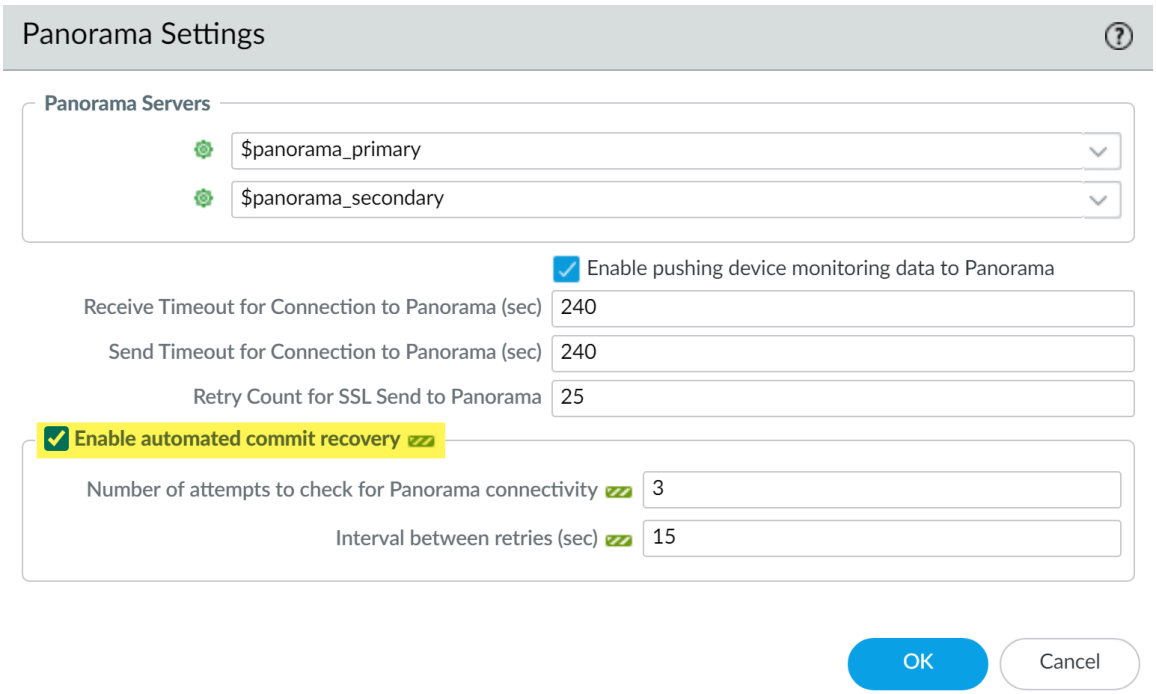
STEP 3 | 자동 커밋 복구를 활성화합니다.

(*ZTP* 방화벽) 자동화된 커밋 복구를 활성화하면 Panorama에 ZTP 방화벽을 추가한 후 초기 구성 푸시가 자동으로 되돌려질 수 있습니다. 관리형 *ZTP* 방화벽에 대해 자동화된 커밋 복구를 활성화하려면 ***Panorama*** 연결 확인 시도 횟수를 ***5***로 구성합니다.

1. 파노라마 설정을 편집(⚙)합니다.
2. 자동 커밋 복구 활성화.
3. **Panorama** 연결 확인 시도 횟수를 구성합니다(기본값은 1회).

(ZTP 방화벽) Panorama에서 처음 푸시한 후 의도하지 않은 구성이 다시 표시되는 것을 방지하려면 시도 횟수를 **5**로 구성합니다.

1. 재시도 간격을 구성합니다(기본값은 10초).
2. 확인을 클릭하여 변경 사항을 저장합니다.



STEP 4 | 커밋 > 커밋하고 푸시하고 변경 사항을 커밋하고 푸시합니다.

STEP 5 | 관리 방화벽에서 자동화된 커밋 복구 기능이 활성화되어 있는지 확인합니다.

1. 방화벽 웹 인터페이스를 시작합니다.
2. 디바이스 > 설정 > 관리를 선택한 다음 Panorama 설정에서 자동 커밋 복구 활성화가 활성화(선택)되었는지 확인합니다.

©2024 Palo Alto Networks, Inc.

Panorama 및 방화벽 구성 백업 관리

Panorama에서 실행 중인 구성은 커밋하여 활성화된 모든 설정으로 구성됩니다. 후보 구성은 실행 중인 구성과 마지막 커밋 이후에 수행한 비활성 변경 사항의 복사본입니다. 실행 중인 구성 또는 후보 구성의 백업 버전을 저장하면 나중에 해당 버전을 복원할 수 있습니다. 예를 들어 커밋 유효성 검사에서 현재 후보 구성에 수정할 것보다 많은 오류가 있음을 보여 주는 경우 이전 후보 구성을 복원할 수 있습니다. 먼저 백업을 저장하지 않고 현재 실행 중인 구성으로 되돌릴 수도 있습니다.

*Panorama*에 구성 변경 사항을 커밋하고 관리형 디바이스에 변경 사항을 푸시하는 방법에 대한 자세한 내용은 Panorama 커밋, 검증 및 미리보기 작업을(를) 참조하십시오.

PAN-OS 5.0 이상의 버전을 실행하는 로컬 방화벽에서 커밋한 후 실행 중인 구성의 백업이 Panorama로 전송됩니다. 관리자가 방화벽에서 로컬로 수행하는 커밋 또는 PAN-OS가 시작하는 자동 커밋(예: FQDN 새로 고침)을 포함하여 로컬 방화벽에서 수행된 모든 커밋은 백업을 트리거합니다. 기본적으로 Panorama는 구성 가능한 각 방화벽에 대해 최대 100개의 백업을 저장합니다. 외부 호스트에 Panorama 및 방화벽 구성 백업을 저장하려면 Panorama에서 내보내기를 예약하거나 요청 시 내보내기를 수행할 수 있습니다. 방화벽에서 Panorama 디바이스 그룹으로 구성을 가져오고 방화벽을 Panorama 관리로 전환(으)로 템플릿을 가져올 수도 있습니다.

(VMware ESXi 및 vCloud Air만 해당) VMware ESXi 및 vCloud Air에 배포된 Panorama 가상 어플라이언스에는 VMware 스냅샷 기능이 지원되지 않습니다. Panorama 가상 어플라이언스의 스냅샷을 생성하면 성능에 영향을 미치고 간헐적이고 일관성 없는 패킷 손실이 발생할 수 있으며 Panorama가 응답하지 않을 수 있습니다. 또한 Panorama CLI 및 웹 인터페이스에 액세스하지 못할 수 있으며 Panorama 모드로의 전환은 지원되지 않습니다. 대신 명명된 구성 스냅샷을 저장하고 네트워크 위치로 내보냅니다.

엔터프라이즈 DLP(데이터 손실 방지)를 활용하는 경우 공유 엔터프라이즈 *DLP* 구성 개체를 포함하지 않는 *Panorama* 구성 백업을 로드하면 엔터프라이즈 *DLP* 기능에 필요한 이러한 공유 객체가 제거됩니다.

- 구성 파일 내보내기 예약
- Panorama 및 방화벽 구성 저장 및 내보내기
- Panorama 구성 변경 사항 되돌리기
- Panorama에서 최대 구성 백업 수 구성
- 관리되는 방화벽에서 구성 백업 로드
- 구성 감사 수행

구성 파일 내보내기 예약

Panorama는 실행 중인 구성의 백업과 모든 관리 방화벽의 실행 중인 구성을 저장합니다. 백업은 일련번호(Panorama 또는 방화벽)를 기반으로 하는 파일 이름이 있는 XML 형식입니다. 이 지침을 사용하여 원격 호스트로 백업을 매일 내보내도록 예약합니다. Panorama는 백업을 단일 gzip 파일로 내보냅니다. 내보내기를 예약하려면 운용 관리자 권한이 필요합니다.

 ©2024 Palo Alto Networks, Inc.

*Panorama*에 고가용성*(HA)* 구성이 있는 경우 각 피어에서 이러한 지침을 수행하여 페일오버 후 예약된 내보내기가 계속되도록 해야 합니다. *Panorama*는 *HA* 피어 간에 예약된 구성 내보내기를 동기화하지 않습니다.

요청 시 백업을 내보내려면 Panorama 및 방화벽 구성 저장 및 내보내기를 참조하십시오.

STEP 1 | (RHEL 서버 버전 8.3만 해당) 버전 8.3을 실행하는 RHEL 서버의 경우 `sshd_config` 파일 내에서 `ChallengeResponseAuthentication` 설정이 **no**인지 확인합니다.

필요한 경우 **no**로 업데이트한 다음 SSH 데몬을 다시 시작합니다. 이 설정은 버전 8.3을 실행하는 RHEL 서버로 구성 파일을 내보내는 데 필요합니다.

STEP 2 | **Panorama** > 예약된 구성 내보내기를 선택한 다음 추가를 클릭합니다.

STEP 3 | 예약된 파일 내보내기에 대한 이름 및 설명을 입력하고 활성화합니다.

STEP 4 | 24시간제 형식을 사용하여 매일 예약된 내보내기 시작 시간을 입력하거나 드롭다운에서 하나를 선택합니다.

둘 이상의 서버에 대한 예약 내보내기를 구성하는 경우 예약 내보내기의 시작 시간을 시차로 설정합니다. 동일한 시작 시간에 여러 내보내기를 예약하면 내보낸 구성 간에 불일치가 발생합니다.

STEP 5 | 내보내기 프로토콜을 **SCP**(Secure Copy) 또는 **FTP**(파일 전송 프로토콜)로 설정합니다.

*Windows*를 실행하는 디바이스로 내보내기는 ***FTP***만 지원합니다.

STEP 6 | 다음을 포함하여 서버 액세스에 대한 세부 정보를 입력합니다. 호스트 이름 또는 IP 주소, 포트, 파일 업로드 경로, 사용자 이름 및 암호.

경로는 **.**(마침표), **+**, **{** 및 **}**, **/**, **-**, **_**, **0-9**, **a-z** 및 **A-Z** 문자를 지원합니다. 파일 경로에는 공백이 지원되지 않습니다.

IPv6 주소를 호스트 이름으로 사용하여 *FTP* 서버로 내보내는 경우 대괄호*([ ])*로 묶인 주소를 입력해야 합니다. 관련 예시로, ***[2001:0db8:0000:0000:0000:8a2e:0370:7334]***가 있습니다.

BSD 서버로 내보내는 경우 *SSHD* 암호 프롬프트를 ***<username>@<hostname> <password>(#)# #### ###***.

STEP 7 | (SCP만 해당) **SCP** 서버 연결 테스트를 클릭합니다. SCP 서버 연결을 테스트하고 안전한 데이터 전송을 활성화하기 위해 일반 텍스트 비밀번호를 입력한 다음 비밀번호 확인을 입력하라는 팝업 창이 표시됩니다.

Panorama는 SCP 서버 비밀번호를 입력하고 확인할 때까지 SCP 서버 연결을 설정하고 테스트하지 않습니다. Panorama에 HA 구성이 있는 경우 각 HA 피어에서 이 단계를 수행하여 각 피어가 SCP 서버의 호스트 키를 수락하도록 합니다. Panorama가 SCP 서버에 성공적으로 연결할 수 있으면 `ssh-export-test.txt`라는 테스트 파일을 생성하고 업로드합니다.

STEP 8 | 확인을 클릭하여 변경 사항을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

Panorama 및 방화벽 구성 저장 및 내보내기

후보 구성의 백업을 Panorama의 영구 스토리지에 저장하면 나중에 해당 백업을 복원할 수 있습니다(Panorama 구성 변경 사항 되돌리기 참조). 또한 Panorama를 사용하면 지정한 디바이스 그룹, 템플릿 및 템플릿 스택(template stack) 구성을 저장하고 내보낼 수 있습니다. 이는 시스템 이벤트 또는 관리자 작업으로 인해 Panorama가 재부팅되는 경우 손실될 변경 사항을 보존하는 데 유용합니다. 재부팅 후 Panorama는 실행 중인 구성의 현재 버전으로 자동으로 되돌아갑니다. 이 구성은 Panorama가 `running-config.xml`이라는 파일에 저장합니다. 백업 저장은 현재 실행 중인 구성보다 이전의 Panorama 구성으로 되돌리려는 경우에도 유용합니다. Panorama는 후보 구성을 영구 저장소에 자동으로 저장하지 않습니다. 후보 구성을 기본 스냅샷 파일(`.snapshot.xml`) 또는 사용자 지정 이름의 스냅샷 파일로 수동으로 저장해야 합니다. Panorama는 스냅샷 파일을 로컬에 저장하지만 외부 호스트로 내보낼 수 있습니다.



마지막 커밋 또는 재부팅 이후의 변경 사항을 되돌리기 위해 구성 백업을 저장할 필요가 없습니다. 구성 > 변경 사항 되돌리기를 선택하기만 하면 됩니다(Panorama 구성 변경 사항 되돌리기 참조).

*Palo Alto Networks*는 중요한 구성을 외부 호스트에 백업할 것을 권장합니다.

STEP 1 | 후보 구성에 대한 변경 사항을 저장합니다.

- 모든 관리자가 수행한 모든 변경 사항으로 기본 스냅샷 파일(`.snapshot.xml`)을 덮어쓰려면 다음 단계 중 하나를 수행합니다.
  - **Panorama** > 설정 > 작업 및 후보 **Panorama** 구성 저장을 선택합니다.
  - 운용 관리자 역할이 할당된 관리 계정 또는 다른 관리자용으로 저장 권한이 활성화된 관리자 역할 프로파일로 Panorama에 로그인합니다. 그런 다음 웹 인터페이스 상단에서 구성 > 변경 사항 저장을 선택한 다음 모든 변경 사항 저장 및 저장을 선택합니다.
- 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성에 대한 관리자의 변경 사항으로 기본 스냅샷(`.snapshot.xml`)을 덮어쓰려면:
  1. **Panorama** > **Setup** > **Operations**, 후보 **Panorama** 구성 저장 및 디바이스 그룹 및 템플릿 선택을 선택합니다.
  2. 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
  3. 확인을 클릭하여 작업을 확인합니다.
  4. (선택 사항) 커밋 > **Panorama**에 커밋를 선택한 다음 변경 사항을 커밋하여 실행 중인 구성을 스냅샷으로 덮어씁니다.
- 기본 스냅샷 파일을 덮어쓰지 않고 모든 관리자가 수행한 모든 변경 사항을 포함하는 스냅샷을 생성하려면:
  1. **Panorama** > 설정 > 작업을 선택하고 명명된 **Panorama** 구성 스냅샷으로 저장됩니다.
  2. 새 구성 파일 또는 기존 구성 파일의 이름을 지정합니다.
  3. 확인을 클릭하고 닫기를 클릭합니다.
- 기본 스냅샷 파일의 일부를 덮어쓰지 않고 후보 구성에 대한 특정 변경 사항만 저장하려면:

 ©2024 Palo Alto Networks, Inc.

1. 원하는 변경 사항을 저장하는 데 필요한 역할 권한이 있는 관리 계정으로 Panorama에 로그인합니다.
2. 웹 인터페이스 상단에서 구성 > 변경 사항 저장을 선택합니다.
3. 변경 사항 저장을 선택합니다.
4. 관리자별로 저장 범위를 필터링하려면을 클릭하고 ***<administrator-name>***을 클릭한 다음 확인을 클릭합니다.
5. 저장 범위를 위치별로 필터링하려면 제외할 위치를 지웁니다. 위치는 특정 디바이스 그룹, 템플릿, 수집기 그룹, 로그 수집기, 공유 설정 또는 Panorama 관리 서버일 수 있습니다.
6. 저장을 클릭하고 새 구성 파일 또는 기존 구성 파일의 이름을 지정한 다음 확인을 클릭합니다.

- 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 저장하려면 다음을 따릅니다.

1. **Panorama** > **Setup** > **Operations**, 명명된 **Panorama** 구성 스냅샷 저장 및 디바이스 그룹 및 템플릿 선택을 선택합니다.
2. 저장할 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
3. 확인을 클릭하여 작업을 확인합니다.

STEP 2 | 후보 또는 실행 중인 구성을 Panorama 외부의 호스트 또는 방화벽으로 내보냅니다.

SCP 또는 FTP 서버로 매일 내보내기를 예약하거나(구성 파일 내보내기 예약 참조) 요청 시 구성을 내보낼 수 있습니다. 요청 시 내보내려면 **Panorama** > **Setup** > **Operations**를 선택한 다음 다음 옵션 중 하나를 선택합니다.

- 명명된 **Panorama** 구성 스냅샷 내보내기 - 현재 실행 중인 구성, 명명된 후보 구성 스냅샷 또는 이전에 불러온 구성(후보 또는 실행 중)을 내보냅니다. Panorama는 사용자가 지정한 이름을 사용하여 구성을 XML 파일로 내보냅니다. 디바이스 그룹 및 템플릿을 선택하여 내보낼 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 지정합니다.
- **Panorama** 구성 버전 내보내기 - 실행 중인 구성의 버전을 선택하여 XML 파일로 내보낼 수 있습니다. 디바이스 그룹 및 템플릿을 선택하여 XML 파일로 내보낼 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 구성을 지정합니다.
- **Panorama** 및 디바이스 구성 번들 내보내기 - Panorama 및 각 관리 방화벽의 실행 중인 구성 백업의 최신 버전을 생성하고 내보냅니다. 구성 번들을 생성하고 매일 SCP(Secure Copy) 또는 FTP 서버로 내보내는 프로세스를 자동화하려면 구성 파일 내보내기 예약을(를) 참조하십시오.
- 디바이스 구성 번들 내보내기 또는 푸시 - 방화벽 구성을 Panorama로 불러온 후 Panorama는 모든 로컬 정책 및 개체가 제거되는 <firewall_name>_import.tg 방화벽 구성 번들을 생성합니다. 그런 다음디바이스 구성 번들을 내보내거나 푸시하여 다음 작업 중 하나를 수행할 수 있습니다.
  - 구성 번들을 방화벽에 푸시 및 커밋하여 로컬 구성을 제거하면 Panorama에서 방화벽을 관리할 수 있습니다.
  - 구성을 로드하지 않고 방화벽으로 내보내기를 합니다. 구성을 로드할 준비가 되면 방화벽 CLI에 로그인하고 구성 모드 명령 **`load device-state`**를 실행합니다. 이 명령은 푸시 및 커밋 옵션과 동일한 방식으로 방화벽을 정리합니다.



방화벽을 Panorama 관리로 전환에 대한 전체 절차에는 추가 단계가 필요합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 구성 변경 사항 되돌리기

변경 사항을 되돌리면 현재 후보 구성의 설정이 다른 구성의 설정으로 바뀝니다. 변경 사항 되돌리기는 각 설정을 수동으로 재구성하는 대신 여러 설정에 대한 변경 사항을 단일 작업으로 실행 취소하려는 경우에 유용합니다.

마지막 커밋 이후 Panorama 구성에 적용된 보류 중인 변경 사항을 되돌릴 수 있습니다. Panorama에서 보류 중인 모든 변경 사항을 되돌리거나 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택할 수 있습니다. Panorama는 관리자 또는 위치별로 보류 중인 변경 사항을 필터링하는 옵션을 제공합니다. 위치는 특정 디바이스 그룹, 템플릿, 수집기 그룹, 로그 수집기, 공유 설정 또는 Panorama 관리 서버일 수 있습니다. 현재 실행 중인 구성보다 이전인 후보 구성에 대한 스냅샷 파일을 저장한 경우(Panorama 및 방화벽 구성 저장 및 내보내기 참조) 해당 후보 구성 스냅샷으로 되돌릴 수도 있습니다. 스냅샷으로 되돌리면 마지막 커밋 이전에 존재했던 후보 구성을 복원할 수 있습니다. Panorama는 변경 사항을 커밋할 때마다 실행 중인 구성의 새 버전을 자동으로 저장하고 해당 버전을 복원할 수 있습니다.

Panorama 관리 서버 구성을 되돌리려면 전체 커밋이 필요하며 운용 관리자가 수행해야 합니다. Panorama 구성 되돌리기 및 로드와 같은 특정 Panorama 작업을 수행할 때 전체 커밋이 필요하며 사용자 지정 관리자 역할 프로파일에는 지원되지 않습니다.

 ©2024 Palo Alto Networks, Inc.

- 현재 Panorama 실행 구성(`running-config.xml` 파일)으로 되돌립니다.

  이 작업은 마지막 커밋 이후 후보 구성에 대한 변경 내용을 취소합니다.

  - 모든 관리자가 변경한 사항을 모두 되돌리려면 다음 단계 중 하나를 수행하십시오.
    - **Panorama** > **Setup** > **Operations**를 선택한 다음 실행 중인 **Panorama** 구성으로 되돌리고 **Yes**를 클릭하여 작업을 확인합니다.
    - 운용 관리자 역할이 할당된 관리 계정 또는 다른 관리자를 위해 커밋 권한이 활성화된 관리자 역할 프로파일로 Panorama에 로그인합니다. 그런 다음 **Config** > **Revert Changes**를 선택한 다음 **Revert All Changes** 및 **Revert**를 선택합니다.
  - 후보 구성에 대한 특정 변경 사항만 되돌리려면:
    1. 원하는 변경 사항을 되돌리는 데 필요한 역할 권한이 있는 관리 계정으로 Panorama에 로그인합니다.

       커밋 작업을 제어하는 권한은 되돌리기 작업도 제어합니다.

    2. **Config** > **Revert Changes**를 선택합니다.
    3. 변경 사항 되돌리기를 선택합니다.
    4. 관리자별로 되돌리기 범위를 필터링하려면 <*administrator-name*>을 클릭하고 관리자를 선택한 다음 확인을 클릭합니다.
    5. 위치별로 되돌리기 범위를 필터링하려면 제외할 위치를 선택 취소합니다.
    6. 변경 사항을 되돌립니다.
  - 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 변경 사항을 실행 중인 구성으로 되돌리려면 다음을 따릅니다.
    1. **Panorama** > **Setup** > **Operations**, 실행 중인 **Panorama** 구성으로 되돌리기, 디바이스 그룹 및 템플릿 선택을 선택합니다.
    2. 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
    3. 확인을 클릭하여 작업을 확인합니다.
    4. (선택 사항) 커밋 > 커밋을 **Panorama**로 선택한 다음 변경 사항 커밋을 선택하여 실행 중인 구성을 덮어씁니다.

 ©2024 Palo Alto Networks, Inc.

- Panorama 후보 구성의 기본 스냅샷(`.snapshots.xml`)으로 되돌립니다.
  - 모든 관리자가 변경한 사항을 모두 되돌리려면 다음을 따릅니다.
    1. **Panorama** > **Setup** > **Operations**를 선택한 다음 마지막으로 저장된 **Panorama** 구성으로 되돌립니다.
    2. 예를 클릭하여 작업을 확인합니다.
    3. (선택 사항) 커밋 > **Panorama**에 커밋를 선택한 다음 변경 사항을 커밋하여 실행 중인 구성을 스냅샷으로 덮어씁니다.
  - 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack) 변경 사항을 실행 중인 구성으로 되돌리려면 다음을 따릅니다.
    1. **Panorama** > **Setup** > **Operations**, 마지막으로 저장된 **Panorama** 구성으로 되돌리기, 디바이스 그룹 및 템플릿 선택을 선택합니다.
    2. 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
    3. 확인을 클릭하여 작업을 확인합니다.
    4. (선택 사항) 실행 중인 구성을 덮어쓰려면 커밋 > **Panorama**에 커밋을 선택한 다음 스냅샷으로 변경 사항을 커밋합니다.

- Panorama에 저장된 실행 중인 구성의 이전 버전으로 되돌립니다.
  - 관리자가 수행한 모든 변경 사항을 되돌리려면 다음을 따릅니다.
    1. **Panorama** > **Setup** > **Operations** 작업, **Panorama** 구성 버전 로드 및 디바이스 그룹 및 템플릿 선택을 선택합니다.
    2. 구성 버전을 선택한 다음 확인을 클릭합니다.
    3. (선택 사항) 실행 중인 구성을 방금 복원한 버전으로 덮어쓰려면 커밋 > **Panorama**에 커밋 및 변경 사항 커밋을 선택합니다.
  - 특정 디바이스 그룹, 템플릿 또는 템플릿 변경 사항을 실행 중인 구성으로 되돌리려면 다음을 따릅니다.
    1. **Panorama** > **Setup** > **Operations**, **Load Panorama** 구성 버전을 선택한 다음 구성 버전 이름을 선택합니다.
    2. 디바이스 그룹 및 템플릿을 선택한 다음 되돌릴 특정 디바이스 그룹, 템플릿 또는 템플릿 스택(template stack)을 선택합니다.
    3. 확인을 클릭하여 작업을 확인합니다.
    4. (선택 사항) 실행 중인 구성을 스냅샷으로 덮어쓰려면 커밋 > **Panorama**에 커밋 및 변경 사항 커밋을 선택합니다.

 ©2024 Palo Alto Networks, Inc.

- 다음 중 하나로 되돌립니다.
  - 이전에 불러온 Panorama 실행 구성의 사용자 지정 이름 버전입니다.
  - 사용자 지정 이름의 Panorama 후보 구성 스냅샷(기본 스냅샷 대신).
    1. **Panorama** > 설정 > 작업를 선택한 다음 이름이 지정된 **Panorama** 구성 스냅샷 로드를 선택하고 방금 불러온 구성 파일의 이름을 선택합니다.
    2. (선택 사항) 공유 개체 로드 또는 공유 정책 로드를 통해 모든 공유 개체 또는 정책을 로드합니다. 모든 공유 개체 및 정책을 로드할 수 있을 뿐만 아니라 다음 단계에서 지정하는 디바이스 그룹 및 템플릿에 구성된 모든 개체 및 정책을 로드할 수 있습니다.
    3. (선택 사항) 디바이스 그룹 및 템플릿을 선택하고 로드할 특정 디바이스 그룹, 템플릿 또는 템플릿 스택 구성을 선택합니다. 전체 Panorama 구성을 되돌리려면 이 단계를 건너뜁니다.
    4. 확인을 클릭하여 작업을 확인합니다.
    5. (선택 사항) 실행 중인 구성을 스냅샷으로 덮어쓰려면 커밋 > **Panorama**에 커밋 및 변경 사항 커밋을 선택합니다.

- 이전에 외부 호스트로 내보낸 실행 중인 Panorama 구성 또는 후보 구성을 복원합니다.
  1. **Panorama** > 설정 > 작업을 선택한 다음 명명된 **Panorama** 구성 스냅샷 가져오기, 외부 호스트에서 구성 파일 찾아보기를 선택하고 확인을 클릭합니다.
  2. 명명된 **Panorama** 구성 스냅샷을 로드하고 방금 불러온 구성 파일의 이름을 선택합니다.
  3. (선택 사항) 공유 개체 로드 또는 공유 정책 로드를 통해 모든 공유 개체 또는 정책을 로드합니다. 모든 공유 개체 및 정책을 로드할 수 있을 뿐만 아니라 다음 단계에서 지정하는 디바이스 그룹 및 템플릿에 구성된 모든 개체 및/또는 정책을 로드할 수 있습니다.
  4. (선택 사항) 디바이스 그룹 및 템플릿을 선택하고 로드할 특정 디바이스 그룹, 템플릿 또는 템플릿 스택 구성을 선택합니다. 전체 Panorama 구성을 되돌리려면 이 단계를 건너뜁니다.
  5. 확인을 클릭하여 작업을 확인합니다.
  6. (선택 사항) 방금 불러온 스냅샷으로 실행 중인 구성을 덮어쓰려면 커밋 > **Panorama**에 커밋 및 변경 사항 커밋을 선택합니다.

Panorama에서 최대 구성 백업 수 구성

STEP 1 | **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.

STEP 2 | 로그 내보내기 및 보고를 선택한 다음 구성 백업의 버전 수를 입력합니다(기본값은 100, 범위는 1~1,048,576).

STEP 3 | 확인을 클릭하여 변경 사항을 저장합니다.

STEP 4 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

관리되는 방화벽에서 구성 백업 로드

Panorama를 사용하여 관리되는 방화벽에서 구성 백업을 로드합니다. 방화벽에 이전에 저장하거나 커밋한 구성으로 되돌리도록 선택할 수 있습니다. Panorama는 선택한 버전을 관리되는 방화벽으로 푸시하여 방화벽의 현재 후보 구성을 덮어씁니다.

 ©2024 Palo Alto Networks, Inc.

STEP 1 | **Panorama** > 관리형 디바이스 > 요약을 선택합니다.

STEP 2 | 백업 열에서 관리를 선택합니다.

STEP 3 | 저장된 구성 또는 커밋된 구성에서 선택합니다.

- 버전 번호를 클릭하면 해당 버전의 내용을 볼 수 있습니다.
- 구성 버전을 로드합니다.

STEP 4 | 방화벽 웹 인터페이스에 로그인하고 변경 사항을 커밋합니다.

구성 감사 수행

구성 감사를 수행하여 구성 변경의 영향을 평가 및 문서화하고, 중단 시 변경 사항을 역추적하고, 보안 규정 준수 표준을 준수하기 위해 정기적인 감사를 수행합니다. active/passive 고가용성(HA) 구성의 Panorama인 경우 ### HA 피어에서만 구성 감사를 수행할 수 있습니다. ## HA 피어에 대한 구성 감사 수행은 지원되지 않습니다.

구성 감사 변경 요약은 최대 25MB 크기의 구성 변경을 지원합니다. 선택한 구성 버전의 구성 변경 크기가 25MB보다 큰 경우 **XML Diff**를 사용할 수 있습니다. 선택한 구성 버전 중 하나에 25MB보다 큰 구성 변경 사항이 있는 경우 변경 요약을 볼 때 경고 메시지가 표시됩니다.

PAN-OS 11.1에서 생성된 커밋 버전에 대해서만 구성 감사를 수행할 수 있습니다. 이전 PAN-OS 릴리즈에서 생성된 커밋 버전은 구성 감사를 지원하지 않습니다.

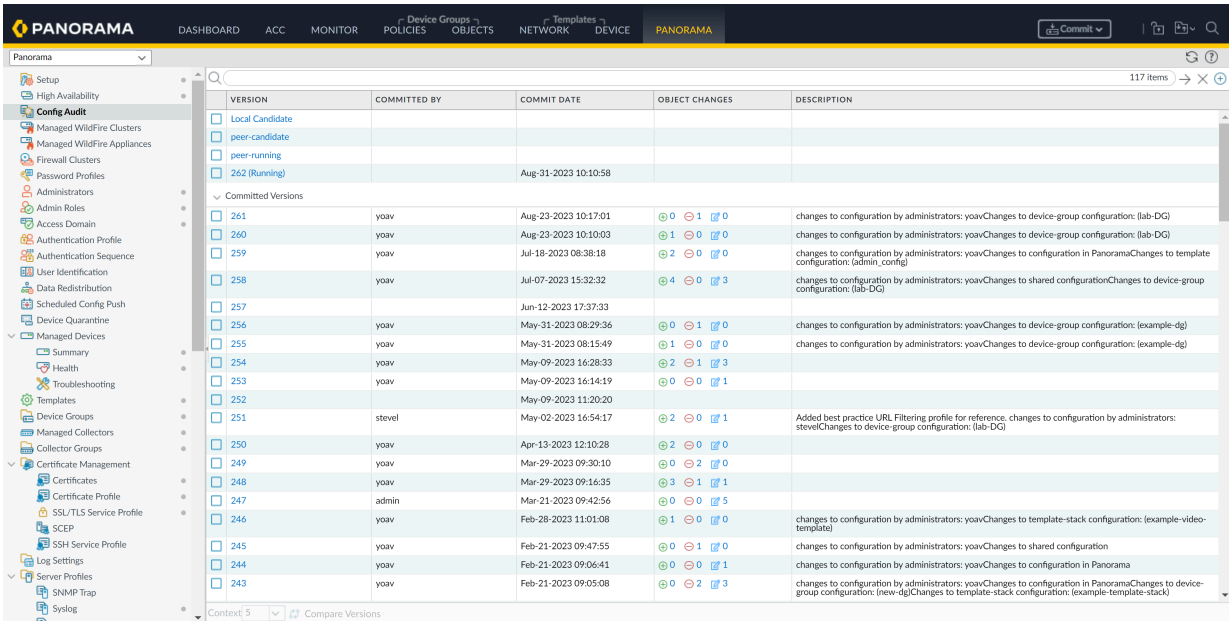
STEP 1 | Panorama 웹 인터페이스에 로그인합니다.

STEP 2 | **Panorama** > 구성 감사를 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 로컬 및 실행 중인 구성 버전, 이전 구성 버전, 저장된 구성 버전에 대한 요약 감사가 표시됩니다.

- 버전 — 특정 커밋의 커밋 버전입니다. 버전은 기본적으로 구성 커밋에 할당되며 순차적입니다.
- 커밋 대상 — 구성 변경을 커밋한 관리자입니다.
- 커밋 날짜 — 구성이 커밋된 날짜 및 시간입니다.
- 개체 — 커밋 버전에서 발생한 구성 변경 사항의 요약입니다. 표시된 구성 변경 요약은 커밋 시 실행 중인 구성을 기준으로 합니다.
  - ⊕ — 새 구성 개체 또는 정책 규칙이 커밋의 일부로 생성되었습니다.
  - ⊖ — 기존 구성 개체 또는 정책 규칙이 커밋의 일부로 삭제되었습니다.
  - 📝 — 기존 구성 개체 또는 정책 규칙이 커밋의 일부로 수정되었습니다.
- 설명 — 추가되면 설명을 커밋합니다.



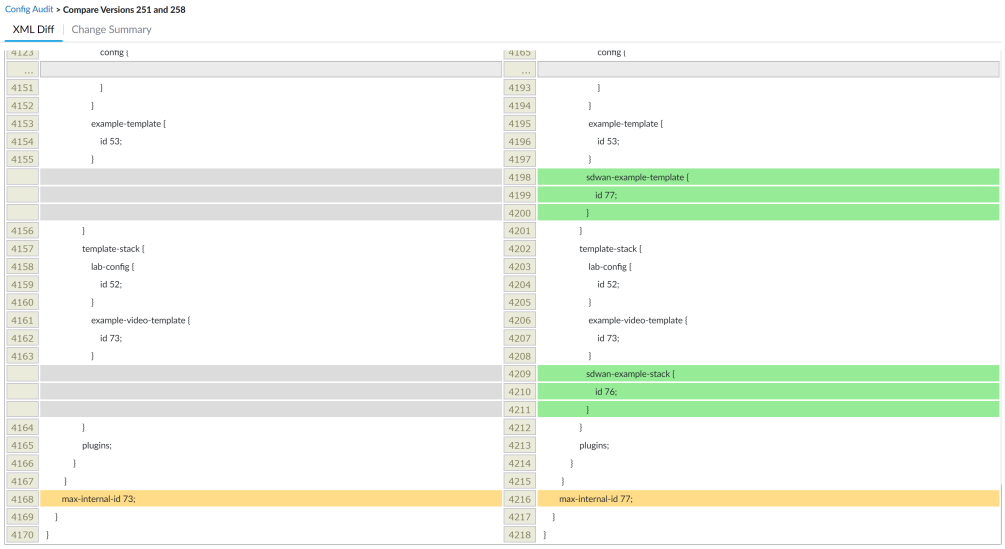
STEP 4 | 최대 두 개의 구성 버전을 선택하고 버전 비교를 선택합니다.

여러 커밋 버전이 있는 두 버전을 선택하면 구성 감사에 가장 오래된 구성 버전과 최근 구성 버전 간의 변경 사항 총계가 표시됩니다. 예를 들어 버전 1과 버전 7을 비교할 때 구성 감사에는 커밋 버전 2~6의 모든 변경 사항도 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | **XML Diff**는 선택한 두 구성 버전 간의 XML 파일 차이점을 나란히 비교하여 표시합니다.

왼쪽 XML은 이전 버전이고 오른쪽 XML은 최신 버전입니다. 녹색으로 강조 표시된 개체는 새로 추가된 구성 개체입니다. 빨간색으로 강조 표시된 개체는 삭제된 구성 개체입니다. 노란색으로 강조 표시된 개체는 수정된 기존 구성 개체입니다.



 ©2024 Palo Alto Networks, Inc.

STEP 6 | 변경 요약에는 선택한 구성 버전과 관련된 구성 개체의 세부 목록이 표시됩니다.

변경 요약 세부 정보를 검토하여 어디에서 어떤 구성 변경이 이루어졌는지 파악하십시오. 특히 ## 열에는 영향을 받은 구성 개체에 대해 수행된 특정 작업이 표시됩니다.

특정 개체 이름을 선택하면 선택한 구성 버전 간의 구성 개체에 대한 개체 레벨 변경 사항을 볼 수 있습니다. 그러면 변경된 내용을 강조 표시하는 XML 스니펫이 표시됩니다.

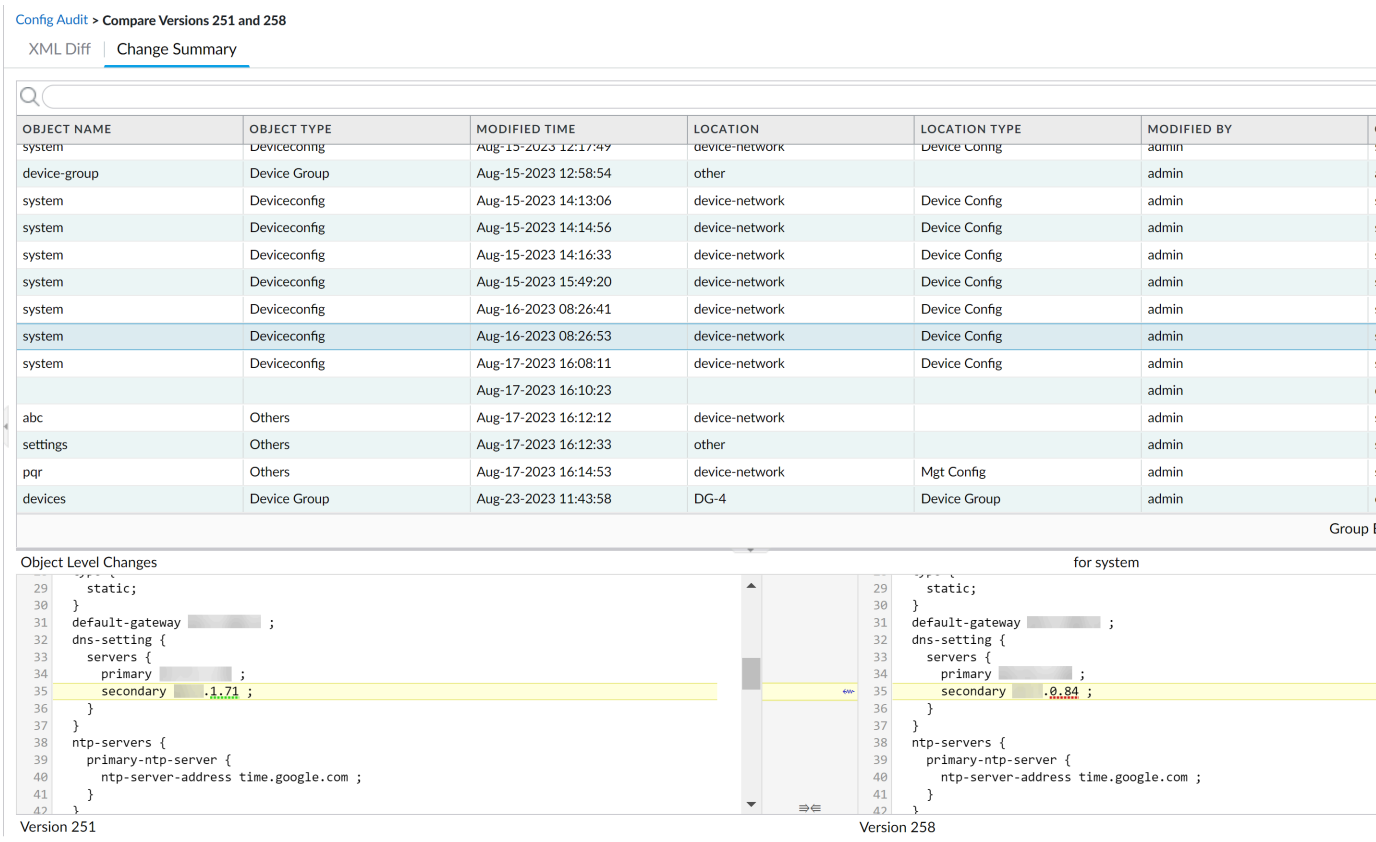
- 설정 — 새 구성 개체가 추가되었습니다.
- 편집 — 기존 구성 개체가 수정되었습니다.
- 이름 변경 — 기존 구성 개체의 이름이 변경되었습니다.
- 이동 — 룰베이스(rulebase) 내에서 정책 규칙을 재정렬하거나 이동합니다.
- 삭제 — 구성 개체가 삭제되었습니다.



다음 작업은 두 개의 개별 작업으로 표시되거나 전혀 표시되지 않을 수 있습니다.

- 기존 구성 개체의 이름을 바꾸는 것은 두 개의 개별 변경 사항으로 표시됩니다. 첫 번째는 이전 이름의 개체에 대한 ***`delete rename`*** 작업입니다. 두 번째는 새 이름을 가진 동일한 개체에 대한 ***`edit create`***입니다.
- 이동 작업은 변경 요약에만 표시됩니다. 이동한 정책 규칙은 ***XML Diff***에 표시되지 않습니다.
- 구성 감사는 로드 및 되돌리기 작업을 캡처할 수 없습니다.
- *(HA만 해당) active/passive* 고가용성*(HA)* 구성의 *Panorama*는 기본 *HA* 피어에서만 구성 감사가 지원됩니다. 보조 *HA* 피어의 웹 인터페이스에서는 구성 감사를 수행할 수 없습니다.

 ©2024 Palo Alto Networks, Inc.



 ©2024 Palo Alto Networks, Inc.

Panorama 구성의 변경 사항 비교

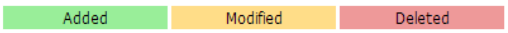
Panorama에서 구성 변경 사항을 비교하려면 후보 구성, 실행 중인 구성 또는 Panorama에서 이전에 저장하거나 커밋한 기타 구성 버전의 두 가지 구성 파일 세트를 선택할 수 있습니다. 병렬 비교를 통해 다음을 수행할 수 있습니다.

- Panorama에 커밋하기 전에 구성 변경 사항을 미리 봅니다. 예를 들어 후보 구성과 실행 중인 구성 간의 변경 사항을 미리 볼 수 있습니다. 가장 좋은 방법은 왼쪽 창에서 이전 버전을 선택하고 오른쪽 창에서 최신 버전을 선택하여 수정 사항을 쉽게 비교하고 식별하는 것입니다.
- 구성 감사를 수행하여 두 구성 파일 세트 간의 변경 사항을 검토하고 비교합니다.

디바이스 그룹 및 템플릿 관리자는 액세스 도메인 내의 디바이스 그룹 및 템플릿에 대한 구성만 비교할 수 있습니다.

- Panorama 구성의 변경 사항을 비교합니다.
  1. **Panorama** > 구성 감사를 선택합니다.
  2. 각 드롭다운에서 비교할 구성을 선택합니다.
  3. 컨텍스트에 포함할 라인 수를 선택하고 실행을 누릅니다.

     Panorama는 색상 음영을 사용하여 추가(녹색), 수정(노란색) 또는 삭제(빨간색) 항목을 강조 표시합니다.



- 구성 감사를 위해 Panorama가 저장하는 버전 수를 구성합니다.
  1. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
  2. 구성 감사의 버전 번호를 입력합니다(범위는 1~1,048,576, 기본값은 100).
  3. 확인을 클릭하여 변경 사항을 저장합니다.
  4. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

- 커밋하기 전에 Panorama 구성 파일을 보고 비교합니다.
  1. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 미리 봅니다.
  2. 보려는 컨텍스트 줄 수를 선택하고 확인을 클릭합니다.

©2024 Palo Alto Networks, Inc.

구성 변경 제한을 위한 잠금 관리

후보를 잠그거나 구성을 실행하면 사용자가 수동으로 잠금을 제거하거나 Panorama가 잠금을 자동으로 제거할 때까지(커밋 후) 다른 관리자가 구성을 변경할 수 없습니다. 잠금은 관리자가 동시 로그인 세션 동안 동일한 설정이나 상호 의존적인 설정에 대해 충돌하는 변경을 하지 않도록 합니다.

동시 세션에서 다른 관리자가 변경하는 설정과 관련이 없는 설정을 변경하는 경우 커밋 충돌을 방지하기 위해 구성 잠금이 필요하지 않습니다. *Panorama*는 커밋 작업을 대기열에 넣고 관리자가 커밋을 시작한 순서대로 수행합니다. 자세한 내용은 Panorama 커밋, 검증 및 미리 보기 작업을(를) 참조하십시오.

템플릿 또는 디바이스 그룹에 할당된 방화벽에 관리자가 해당 방화벽에서 로컬로 설정한 커밋 또는 구성 잠금이 있는 경우 템플릿 또는 디바이스 그룹 구성 푸시가 실패합니다.

- 현재 잠금에 대한 세부 정보를 봅니다.

  예를 들어 다른 관리자가 잠금을 설정했는지 확인하고 잠금을 설명하기 위해 입력한 설명을 읽을 수 있습니다.

  웹 인터페이스 상단의 잠긴 자물쇠()를 클릭합니다. 인접한 숫자는 현재 잠금 수를 나타냅니다.

- 구성을 잠급니다.

  방화벽 또는 Panorama 구성을 수정할 수 없는 읽기 전용 관리자는 잠금을 설정할 수 없습니다.

  1. 웹 인터페이스 상단의 자물쇠 아이콘을 클릭합니다.

     아이콘은 기존 잠금이 설정되었는지() 설정되지 않았는지()에 따라 다릅니다.
  2. 잠금을 선택하고 잠금 유형을 선택합니다.
     - 구성 - 다른 관리자가 후보 구성을 변경하지 못하도록 차단합니다.

       변경 사항을 커밋할 수 없는 사용자 지정 역할 관리자는 구성 잠금을 설정하고 변경 사항을 후보 구성에 저장할 수 있습니다. 그러나 해당 관리자는 변경 사항을 커밋할 수 없기 때문에 *Panorama*는 커밋 후에 자동으로 잠금을 해제하지 않습니다. 관리자는 필요한 변경을 수행한 후 구성 잠금을 수동으로 제거해야 합니다.

     - 커밋 - 다른 관리자가 실행 중인 구성을 변경하지 못하도록 차단합니다.
  3. 위치를 선택하여 잠금 범위를 결정합니다.
     - 공유 - 모든 디바이스 그룹 및 템플릿을 포함하여 전체 Panorama 구성에 대한 변경을 제한합니다.
     - 템플릿 - 선택한 템플릿에 포함된 방화벽에 대한 변경을 제한합니다. (템플릿 스택(template stack)에 대해 잠금을 설정할 수 없으며 스택 내의 개별 템플릿에 대해서만 잠금을 설정할 수 있습니다.)
     - 디바이스 그룹 - 선택한 디바이스 그룹에 대한 변경을 제한하지만 하위 디바이스 그룹은 제한하지 않습니다.
  4. (선택 사항) 모범 사례로 설명을 입력하여 잠금 설정 이유를 설명합니다.
  5. 확인을 클릭하고 닫기를 클릭합니다.

©2024 Palo Alto Networks, Inc.

- 구성을 잠금 해제합니다.

  구성을 잠근 운용 관리자 또는 관리자만 수동으로 잠금을 해제할 수 있습니다. 그러나 Panorama는 잠금을 설정한 관리자가 시작한 커밋 작업을 완료한 후 자동으로 잠금을 제거합니다.

  1. 웹 인터페이스 상단의 잠긴 자물쇠()를 클릭합니다.
  2. 목록에서 잠금 항목을 선택합니다.
  3. 잠금 제거, 확인, 닫기를 차례로 클릭합니다.

- 후보 구성을 변경할 때 실행 중인 구성을 자동으로 잠그도록 Panorama를 구성합니다. 이 설정은 모든 Panorama 관리자에게 적용됩니다.

  1. **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.
  2. 커밋 잠금 자동 획득을 선택한 다음 확인을 클릭합니다.
  3. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.

©2024 Palo Alto Networks, Inc.

Panorama에 사용자 정의 로고 추가

이미지 파일을 업로드하여 Panorama의 다음 영역을 사용자 지정할 수 있습니다.

- 로그인 화면의 배경 이미지
- 웹 인터페이스의 왼쪽 상단 모서리에 있는 헤더; Panorama 기본 배경을 숨길 수도 있습니다.
- PDF 보고서의 제목 페이지 및 풋터 이미지

지원되는 이미지 유형에는.jpg 및.png가 있습니다. PDF 보고서에 사용할 이미지 파일에는 알파 채널이 포함될 수 없습니다. 이미지의 크기는 128킬로바이트(131,072바이트)보다 작아야 합니다. 권장 치수가 화면에 표시됩니다. 치수가 권장 크기보다 크면 이미지가 자동으로 자른다.

비인터레이스 이미지만 지원됩니다. 이메일로 전송된 예약 보고서 및 지금 실행 사용자 정의 보고서는 사용자 정의 인터레이스 이미지가 *PDF* 보고서 제목 또는 *PDF* 보고서 헤더에 포함된 경우 *PDF* 첨부 파일을 포함하지 않습니다.

STEP 1 | **Panorama** > 설정 > 작업을 선택합니다.

STEP 2 | 기타 섹션에서 사용자 정의 로고를 클릭합니다.

STEP 3 | 업로드 로고 아이콘을 클릭하고 로그인 화면, 기본 사용자 인터페이스의 왼쪽 모서리, PDF 보고서 제목 페이지 및 PDF 보고서 푸터와 같은 다음 옵션에 대한 이미지를 선택합니다.

STEP 4 | 이미지를 추가하려면 열기를 클릭합니다. 이미지를 미리 보려면 미리보기 로고 아이콘을 클릭합니다.

STEP 5 | (선택 사항) Panorama 웹 인터페이스에서 녹색 배경 헤더를 지우려면 **Panorama** 백그라운드 헤더 제거의 확인란을 선택합니다.

STEP 6 | 변경 내용을 저장하려면 닫기를 클릭합니다.

STEP 7 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 작업 관리자 사용

웹 인터페이스 하단의 작업(Tasks)을 클릭하여 관리자가 시작한 모든 작업(예: 수동 커밋) 또는 Panorama 또는 관리되는 방화벽(예: 예약된 보고서 생성)에 대한 세부 정보를 표시하는 작업 관리자를 엽니다. 작업 관리자를 사용하여 실패한 작업을 해결하거나, 완료된 커밋과 관련된 경고를 조사하거나, 보류 중인 커밋을 취소할 수 있습니다.

디바이스 그룹 및 템플릿 관리자는 액세스 도메인 내에서 작업에 대한 작업만 볼 수 있습니다.

STEP 1 | 작업을 클릭합니다.

STEP 2 | 실행 중(진행 중인) 작업 또는 모든 작업(기본값)을 표시하고 선택적으로 유형별로 필터링합니다(보고서, 로그 요청, 작업을 커밋, 다운로드 및 설치하고 **Panorama**(기본값) 또는 작업을 보려는 방화벽을 선택합니다.

STEP 3 | 다음 작업 중 하나를 수행합니다.

- 작업 세부 정보 표시 또는 숨기기 - 기본적으로 작업 관리자는 각 작업에 대한 유형, 상태, 시작 시간 및 메시지를 표시합니다. 작업에 대한 종료 시간 및 작업 ID를 보려면 해당 열을 수동으로 표시해야 합니다. 열을 표시하거나 숨기려면 열 헤더에서 드롭다운을 열고 열을 선택한 다음 원하는 대로 열을 선택하거나 지웁니다.
- 경고 또는 실패를 조사합니다—작업 세부 사항에 대한 메시지 열의 항목을 읽으십시오. 열에 `Toomany ###`가 표시되면 형식 열의 항목을 클릭하여 자세한 내용을 확인합니다.
- 커밋 설명 표시—관리자가 커밋에 대한 설명을 입력한 경우 메시지 열에서 커밋 설명을 클릭하여 표시합니다.
- 큐에서 커밋의 위치를 확인합니다—메시지열은 진행 중인 커밋의 큐 위치를 나타냅니다.
- 보류 중인 커밋 취소-보류 중인 모든 커밋을 취소하려면 커밋 대기열을 지웁니다(사전 정의된 관리 역할에만 사용 가능). 개별 커밋을 취소하려면 작업 열에서 **x**를 클릭합니다(Panorama가 큐에 대기할 때까지 커밋이 큐에 남아 있음). 진행 중인 커밋을 취소할 수 없습니다.

©2024 Palo Alto Networks, Inc.

로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 관리

- 로그 및 보고서 저장소
- 로그 및 보고서 만료 기간
- 로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 구성
- Panorama 보고서의 실행 시간 구성

로그 및 보고서 저장소

각 로그 유형에 대한 기본 저장소 할당량을 편집할 수 있습니다. 로그 할당량이 최대 크기에 도달하면 Panorama는 가장 오래된 로그 항목을 새 로그 항목으로 덮어쓰기 시작합니다. 보고서의 저장 용량은 구성할 수 없습니다. 로그 저장 위치 및 보고서 저장 용량은 Panorama 모델에 따라 다릅니다.

- **Panorama** 모드의 **Panorama** 가상 어플라이언스 - 보고서 저장 공간은 200MB입니다. 어플라이언스는 가상 시스템 디스크를 사용하여 Panorama 및 로그 수집기가 생성하는 시스템 및 구성 로그를 저장합니다. 가상 시스템 디스크는 또한 Panorama가 관리되는 모든 방화벽에서 15분 간격으로 자동으로 수신하는 애플리케이션 통계(앱 통계) 로그를 저장합니다. Panorama는 다른 모든 로그 유형을 가상 로깅 디스크(1~12)에 저장합니다.
- 관리 전용 모드의 **Panorama** 가상 어플라이언스 - 보고서의 저장 공간은 500MB입니다. 어플라이언스는 가상 시스템 디스크를 사용하여 Panorama 및 로그 수집기가 생성하는 시스템 및 구성 로그를 저장합니다. 가상 시스템 디스크는 또한 Panorama가 관리되는 모든 방화벽에서 15분 간격으로 자동으로 수신하는 애플리케이션 통계(앱 통계) 로그를 저장합니다. 관리 전용 모드의 Panorama는 다른 로그 유형을 저장할 수 없으므로 관리 방화벽의 로그를 포워딩하려면 관리 수집기를 구성해야 합니다.
- 레거시 모드의 **Panorama** 가상 어플라이언스 - 보고서의 저장 공간은 Panorama 8.0 이하 버전의 경우 200MB이고 Panorama 8.0.1 이상의 버전의 경우 500MB입니다. Panorama는 다음 중 하나일 수 있는 할당된 저장 공간에 모든 로그를 기록합니다.
  - 가상 시스템 디스크 - 기본적으로 Panorama를 설치할 때 생성한 가상 시스템 디스크의 로그 스토리지에 약 11GB가 할당됩니다. 가상 로깅 디스크 또는 NFS 파티션을 추가하는 경우 Panorama는 여전히 시스템 디스크를 사용하여 Panorama 및 로그 수집기가 생성하는 시스템 및 구성 로그를 저장하고 방화벽에서 수집된 앱 통계 로그를 저장합니다.
  - 전용 가상 로깅 디스크 - 시스템 디스크에 있는 로그 유형을 제외한 모든 로그 유형을 저장합니다.
  - **NFS** 파티션 - 이 옵션은 VMware ESXi 서버에서 실행되는 Panorama에만 사용할 수 있습니다. NFS 파티션은 시스템 디스크에 있는 로그 유형을 제외한 모든 로그 유형을 저장합니다.
- **M-700, M-600, M-500, M-300** 또는 **M-200** 어플라이언스 - 보고서의 저장 공간은 Panorama 6.1 이상 릴리스의 경우 500MB, 이전 릴리스의 경우 200MB입니다. M 시리즈 어플라이언스는 내부 SSD를 사용하여 Panorama 및 로그 수집기가 생성하는 구성 로그 및 시스템 로그를 저장하고 방화벽에서 수집된 앱 통계 로그를 저장합니다. Panorama는 다른 모든 로그 유형을 RAID 지원 디스크에 저장합니다. RAID 디스크는 Panorama 모드의 M-시리즈 어플라이언스에 로컬이거나 전용 로그 수집

 ©2024 Palo Alto Networks, Inc.

기(로그 수집기 모드의 M-시리즈 어플라이언스)에 있습니다. 수집기 그룹을 구성할 때 RAID 디스크의 로그 저장소 할당량을 편집합니다.

로그 저장 옵션 및 용량에 대한 자세한 내용은 Panorama 모델을 참조하십시오. 가상 로깅 디스크 또는 *NFS* 스토리지를 추가하여 Panorama 가상 어플라이언스에서 로그 스토리지 용량을 확장할 수 있습니다. *RAID* 드라이브를 추가하거나 *1TB* 드라이브에서 *2TB* 드라이브로 업그레이드하여 M-시리즈 어플라이언스의 스토리지를 늘릴 수 있습니다.

로그 및 보고서 만료 기간

Panorama 관리 서버 및 로그 수집기가 방화벽에서 수집하는 로그는 물론 Panorama 및 로그 수집기가 로컬에서 생성하는 로그 및 보고서에 대한 시간을 기반으로 자동 삭제를 구성할 수 있습니다. 이는 모니터링되는 정보를 주기적으로 삭제해야 하거나 필요한 배포에 유용합니다. 예를 들어, 특정 기간이 지난 후 사용자 정보를 삭제하는 것은 법적 이유로 조직에서 필수일 수 있습니다. 다음에 대해 별도의 만료 기간을 구성합니다.

- 보고서 - Panorama는 새 보고서를 생성함과 동시에 만료된 보고서를 삭제합니다(Panorama 보고서의 런타임 구성 참조).
- 각 로그 유형 - Panorama는 수신된 로그를 평가하고 구성된 만료 기간을 초과하는 로그를 삭제합니다.
- *Panorama*는 고가용성*(HA)* 쌍 간에 만료 기간을 동기화합니다. 활성 *HA* 피어만 로그를 생성하기 때문에 패시브 피어는 페일오버가 발생하고 로그 생성을 시작하지 않는 한 삭제할 로그나 보고서가 없습니다.

  만료 기간을 설정하지 않은 경우에도 로그 할당량이 최대 크기에 도달하면 *Panorama*는 가장 오래된 로그 항목을 새 로그 항목으로 덮어쓰기 시작합니다.

로그 및 보고서에 대한 스토리지 할당량 및 만료 기간 구성

 ©2024 Palo Alto Networks, Inc.

STEP 1 | 다음에 대한 스토리지 할당량 및 만료 기간을 구성합니다.

- 레거시 모드의 Panorama 가상 어플라이언스가 방화벽에서 수신하는 모든 유형의 로그입니다.
- Panorama가 방화벽에서 수신하는 앱 통계 로그입니다.
- Panorama 및 Log Collectors가 로컬에서 생성하는 시스템 및 구성 로그.

Panorama 관리 서버는 이러한 로그를 로컬에 저장합니다.

현재 로그가 초과하도록 스토리지 할당량을 줄이면 변경 사항을 커밋한 후 *Panorama*가 할당량에 맞게 가장 오래된 로그를 제거합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.
2. 로그 저장소 설정에서 각 로그 유형에 대한 저장소 할당량**(%)**을 입력합니다.

   백분율 값을 변경하면 Panorama에 할당된 총 스토리지를 기반으로 해당 절대 값(Quota GB/MB 열)을 표시하도록 페이지가 새로 고쳐집니다.
3. 각 로그 유형(범위는 1~2,000)에 대한 최대 일수(만료 기간)를 입력합니다.

   기본적으로 필드는 비어 있으므로 로그가 만료되지 않습니다.

   할당량 및 만료 기간을 공장 기본값으로 재설정하려면 기본값 복원을 선택합니다.

STEP 2 | Panorama가 생성하는 보고서의 만료 기간을 구성합니다.

1. 로그 내보내기 및 보고를 선택한 다음 보고서 만료 기간을 일 단위로 입력합니다(범위는 1 - 2,000).

   기본적으로 필드는 비어 있으므로 보고서가 만료되지 않습니다.
2. 확인을 클릭하여 변경 사항을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | M-700, M-600, M-500, M-300, M-200 어플라이언스 또는 Panorama 모드의 Panorama 가상 기기가 방화벽에서 수신하는 모든 유형의 로그(App Stats 로그 제외)에 대한 스토리지 할당량 및 만료 기간을 구성합니다.

로컬 또는 전용 로그 수집기는 이러한 로그를 저장합니다.

개별 로그 수집기가 아닌 수집기 그룹 수준에서 이러한 저장소 할당량을 구성합니다.

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 편집합니다.
2. 일반 설정에서 로그 저장소 값을 클릭합니다.

   수집기 그룹에 로그 수집기를 할당하지 않으면 값이 표시되지 않습니다. 로그 수집기를 할당한 후 필드에 *0MB*가 표시되면 관리형 수집기를 구성할 때 디스크 쌍을 활성화하고 변경 사항을 커밋했는지 확인합니다(***Panorama*** > 관리형 수집기 > 디스크).
3. 각 로그 유형에 대한 스토리지 할당량**(%)**을 입력합니다.

   백분율 값을 변경하면 페이지가 새로 고쳐지고 Collector Group에 할당된 총 스토리지를 기반으로 해당 절대값(Quota GB/MB 열)이 표시됩니다.
4. 각 로그 유형(범위는 1~2,000)에 대한 최대 일수(만료 기간)를 입력합니다.

   기본적으로 필드는 비어 있으므로 로그가 만료되지 않습니다.

   할당량 및 만료 기간을 공장 기본값으로 재설정하려면 기본값 복원을 선택합니다.
5. 확인을 클릭하여 변경 사항을 저장합니다.

STEP 4 | Panorama에 변경 사항을 커밋하고 Collector Group에 변경 사항을 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 수집기 그룹을 선택한 다음 수정한 수집기 그룹을 선택한 다음 확인을 클릭합니다.
3. 변경 사항을 커밋하고 푸시합니다.

STEP 5 | Panorama가 스토리지 할당량 변경 사항을 적용했는지 확인합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정에서 Panorama 관리 서버가 저장하는 로그에 대한 로그 저장소 값이 올바른지 확인합니다.
2. **Panorama** > 수집기 그룹을 선택한 다음 수정한 수집기 그룹을 선택한 다음 일반 탭의 로그 스토리지 값이 로그 수집기가 저장하는 로그에 대해 올바른지 확인합니다.

   *Log Collector CLI*에 로그인하고 ***show log-diskquota-pct*** 운영 명령을 입력하여 *Collector Group* 스토리지 할당량을 확인할 수도 있습니다.

Panorama 보고서의 실행 시간 구성

Panorama는 매일 지정한 시간에 보고서를 생성합니다. Panorama는 새 보고서를 생성한 후 만료된 보고서를 삭제합니다.

STEP 1 | **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 로그 내보내기 및 보고를 선택한 다음 보고서 런타임을 24시간 단위의 일정에서 한 시간으로 설정합니다(기본값은 02:00, 범위는 00:00[자정]~23:00).

STEP 3 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

모니터 Panorama

Panorama 및 관리되는 수집기를 모니터링하려면 시스템 및 구성 로그를 주기적으로 보고(유형별로 로그 필터링), 정기적으로 Panorama 통계를 수집(GET)하도록 SNMP 관리자를 구성하거나, 모니터링된 지표가 Panorama에서 상태를 변경하거나 임계값에 도달할 때 사용자에게 알리는 SNMP 트랩 또는 이메일 경고를 구성할 수 있습니다. 이메일 경고 및 SNMP 트랩은 주의가 필요한 중요한 시스템 이벤트에 대한 즉각적인 알림에 유용합니다. 이메일 경고 또는 SNMP 트랩을 구성하려면 Panorama에서 외부 대상으로 로그 포워딩 구성을(를) 참조하십시오.

- Panorama 시스템 및 구성 로그
- SNMP를 사용하여 Panorama 및 로그 수집기 통계 모니터링

Panorama 시스템 및 구성 로그

시스템 이벤트 또는 구성 변경이 발생할 때 알림을 보내도록 Panorama를 구성할 수 있습니다. 기본적으로 Panorama는 구성 로그에 모든 구성 변경 사항을 기록합니다. 시스템 로그에서 각 이벤트에는 긴급성과 영향을 나타내는 심각도 수준이 있습니다. Panorama에서 외부 대상으로 로그 포워딩 구성을(를) 하면 모든 시스템 및 구성 로그를 포워딩하거나 수신 시간 또는 심각도 수준(시스템 로그만)과 같은 속성을 기반으로 로그를 필터링할 수 있습니다. 다음 표에는 시스템 로그의 심각도 수준이 요약되어 있습니다.

*Panorama*는 정기적으로 *IoT Edge* 서비스에 연결하여 *IoT* 기반 정책에 대한 정책 권장 사항을 다운로드합니다. 이 연결은 관리형 방화벽에서 *IoT* 라이선스가 활성화되어 있는지 여부에 관계없이 *Panorama*에서 시도합니다.

연결 실패가 발생하거나 *Panorama*가 *IoT* 라이선스 방화벽을 관리하지 않는 경우 심각도가 높은 *gRPC* 연결 실패 시스템 로그가 생성됩니다. *IoT*의 정책 권장 사항 기능을 활용하지 않거나 *IoT* 라이선스 방화벽을 관리하지 않는 경우 이러한 시스템 로그에 대해 조치가 필요하지 않습니다.

*IoT*의 정책 권장 사항 기능을 활용하는 경우 *gRPC* 연결 실패 시스템 로그를 검토하여 *Panorama*와 *IoT Edge* 서비스 간의 연결 문제를 일으키는 원인을 파악하세요.

*Panorama*는 ***ACC***에서 구성 로그 쿼리를 지원하지 않거나 필터를 사용하여 구성 로그(***Monitor > Logs***)를 모니터링할 때 지원하지 않습니다.

before-change-preview-contains

after-change-preview-contains

심각성	설명
심각함	장애 및 고가용성(HA) 페일오버 및 링크 장애를 포함한 하드웨어 장애와 같은 즉각적인 주의가 필요한 사항을 나타냅니다.

©2024 Palo Alto Networks, Inc.

심각성	설명
높음	로그 수집기 연결 해제 또는 커밋 실패를 포함하여 시스템 작동을 손상시키는 심각한 문제.
중간	바이러스 백신 패키지 업그레이드 또는 수집기 그룹 구성 푸시와 같은 중간 수준 알림.
낮음	사용자 암호 변경과 같은 사소한 심각도 알림.
정보 제공	로그인 또는 로그아웃, 구성 변경, 인증 성공 및 실패 알림, 커밋 성공 및 기타 심각도 수준에서 다루지 않는 기타 모든 이벤트와 같은 알림 이벤트.

Panorama는 시스템 및 구성 로그를 로컬에 저장합니다. 정확한 위치와 저장 용량은 Panorama 모델에 따라 다릅니다(로그 및 보고서 저장소 참조). 용량 제한에 도달하면 Panorama는 가장 오래된 로그를 삭제하여 새 로그를 위한 공간을 생성합니다. 로컬 저장소가 허용하는 것보다 더 오랜 기간 동안 로그를 저장해야 하는 경우 Panorama에서 외부 대상으로 로그 포워딩 구성을(를) 할 수 있습니다.

*Panorama*를 사용하여 방화벽 로그를 모니터링하는 방법에 대한 자세한 내용은 네트워크 활동 모니터링을(를) 참조하십시오.

SNMP를 사용하여 Panorama 및 로그 수집기 통계 모니터링

Panorama 관리 서버에서 정보를 요청하도록 SNMP 관리자를 구성하고 응답하도록 Panorama를 구성할 수 있습니다. 예를 들어 SNMP 관리자는 고가용성(HA) 모드, Panorama 상태 및 Panorama 버전을 요청할 수 있습니다. Panorama 관리 서버에 로컬 로그 수집기가 있는 경우, Panorama는 초당 평균 로그, 저장 기간, 보존 기간, 로그 디스크 사용량, 개별 방화벽에서 Panorama 및 외부 서버로의 로그 포워딩 상태, 방화벽-로그 수집기 연결 상태에 대한 로깅 통계를 제공할 수도 있습니다. Panorama는 HA 피어 간에 SNMP 구성을 동기화하지 않습니다. 각 피어에서 SNMP 요청 및 응답을 활성화해야 합니다.

Panorama 관리 서버와 동일한 로깅 통계에 대한 요청에 응답하도록 전용 로그 수집기를 구성할 수도 있습니다. 이 정보는 로그 스토리지 용량을 확장해야 하는지의 여부를 평가할 때 유용합니다.

SNMP 관리자를 구성하여 *Panorama* 또는 로그 수집기를 제어할 수 없습니다*(SET* 메시지 사용*). SNMP* 관리자는 *GET* 메시지를 사용하여 통계만 수집할 수 있습니다.

*Panorama*가 *SNMP*를 구현하는 방법에 대한 자세한 내용은 SNMP 지원을 참조하십시오.

STEP 1 | Panorama 및 로그 수집기에서 통계를 가져오도록 SNMP 관리자를 구성합니다.

다음 단계는 SNMP 관리자에서 수행하는 작업의 개요입니다. 특정 단계의 경우 SNMP 관리자의 설명서를 참조하십시오.

1. SNMP 관리자가 통계를 해석할 수 있도록 하려면 지원되는 MIB를 로드하고 필요한 경우 컴파일합니다.
2. SNMP 관리자가 모니터링할 각 Panorama 어플라이언스에 대해 연결 설정(IP 주소 및 포트) 및 인증 설정(SNMPv2c 커뮤니티 문자열 또는 SNMPv3 사용자 이름 및 비밀번호)을 정의합니다. 모든 Panorama 어플라이언스는 포트 161을 사용합니다.

 ©2024 Palo Alto Networks, Inc.

SNMP 관리자는 여러 Panorama 관리 서버 및 로그 수집기에 대해 동일하거나 다른 연결 및 인증 설정을 사용할 수 있습니다. 설정은 Panorama에서 SNMP를 구성할 때 정의한 설정과 일치해야 합니다(SNMP 관리자의 통계 요청에 응답하도록 Panorama 관리 서버 구성 및 SNMP 관리자의 통계 요청에 응답하도록 Panorama 관리 서버 구성 참조). 예를 들어, SNMPv2c를 사용하는 경우 Panorama를 구성할 때 정의하는 커뮤니티 문자열은 Panorama용 SNMP 관리자에서 정의한 커뮤니티 문자열과 일치해야 합니다.

3. 모니터링할 통계의 개체 식별자(OID)를 결정합니다. 예를 들어, 로깅 속도를 모니터링하기 위해 MIB 브라우저는 이 통계가 PAN-PRODUCT-MIB.my의 OID 1.3.6.1.4.1.25461.2.3.30.1.1에 해당함을 보여줍니다. 자세한 내용은 SNMP 관리자를 사용하여 MIB 및 개체를 탐색하는 방법을 참조하십시오.
4. 원하는 OID를 모니터링하도록 SNMP 관리자를 구성합니다.

STEP 2 | Panorama 관리 서버의 관리(MGT) 인터페이스에서 SNMP 트래픽을 활성화합니다.

1. **Panorama** > 설정 > 관리를 선택한 다음 관리 인터페이스 설정을 편집합니다.
2. 서비스 섹션에서 **SNMP** 확인란을 선택한 다음 확인을 클릭합니다.

STEP 3 | Log Collector 모드에서 M-시리즈 어플라이언스의 관리(MGT) 인터페이스에서 SNMP 트래픽을 활성화합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 로그 수집기를 선택합니다.
2. 관리 탭을 선택한 다음 **SNMP** 확인란을 선택하고 확인을 클릭합니다.

STEP 4 | SNMP 관리자의 통계 요청에 응답하도록 Panorama 관리 서버를 구성합니다.

1. **Panorama** > 설정 > 작업을 선택한 다음 기타 섹션에서 **SNMP** 설정을 클릭합니다.
2. SNMP 버전을 선택하고 인증 값을 다음과 같이 구성합니다. 버전 세부 정보는 SNMP 지원을 참조하십시오.

   - **V2c** - SNMP 관리자 및 모니터링되는 디바이스(이 경우 Panorama)의 커뮤니티를 식별하고 커뮤니티 구성원을 서로 인증하기 위한 암호 역할을 하는 **SNMP** 커뮤니티 문자열을 입력합니다.

     기본 커뮤니티 문자열 ***public***을 사용하지 마십시오. 일반적으로 알려져 있으므로 안전하지 않습니다.

   - **V3** - 하나 이상의 SNMP 보기 그룹과 하나의 사용자를 생성합니다. 사용자 계정 및 보기는 SNMP 관리자가 통계를 얻을 때 인증, 개인 정보 보호 및 액세스 제어를 제공합니다.

     보기 - 각 보기는 쌍을 이루는 OID와 비트 단위 마스크입니다. OID는 MIB를 지정하고 마스크(16진수 형식)는 해당 MIB 내부(일치 포함) 또는 외부(일치 제외)에 액세스할 수 있는 객체를 지정합니다. 첫 번째 목록에서 추가를 클릭하고 보기 그룹의 이름을 입력합니다. 그룹의 각 보기에 대해 추가를 클릭하고 보기 이름, **OID**, 일치 옵션(포함 또는 제외) 및 마스크를 구성합니다.

     사용자 - 두 번째 목록에서 추가를 클릭하고 사용자 열에 사용자 이름을 입력하고 드롭다운에서 보기 그룹을 선택한 다음 SNMP 관리자를 인증하는 데 사용되는 인증 암호(인증 암호)를 입력하고 개인 정보 암호(**Priv** 암호) SNMP 관리자에 대한 SNMP 메시지를 암호화하는 데 사용됩니다.
3. 확인을 클릭하여 설정을 저장합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | SNMP 요청에 응답하도록 전용 로그 수집기(있는 경우)를 구성합니다.

각 수집기 그룹에 대해:

1. **Panorama** > 수집기 그룹을 선택한 다음 수집기 그룹을 선택합니다.
2. 모니터링 탭을 선택한 다음 SNMP 관리자의 통계 요청에 응답하도록 Panorama 관리 서버 구성 단계에서와 동일한 설정을 구성하고 확인을 클릭합니다.

STEP 6 | Panorama에 변경 사항을 커밋하고 Collector Groups에 변경 사항을 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 수집기 그룹을 선택한 다음 편집한 수집기 그룹을 선택한 다음 확인을 클릭합니다.
3. 변경 사항을 커밋하고 푸시합니다.

STEP 7 | SNMP 관리자에서 Panorama 및 로그 수집기 통계를 모니터링합니다.

SNMP 관리자의 설명서를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

Panorama 재부팅 또는 종료

재부팅 옵션은 Panorama의 정상적인 재시작을 시작합니다. 시스템을 종료하면 시스템이 중지되고 전원이 꺼집니다. Panorama를 다시 시작하려면 시스템을 종료한 후 시스템의 전원 코드를 수동으로 분리했다가 다시 연결하십시오.

STEP 1 | **Panorama** > 설정 > 작업을 선택합니다.

STEP 2 | 디바이스 작업 섹션에서 **Panorama** 재부팅 또는 **Panorama** 종료를 선택합니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 암호 프로파일 및 복잡성 구성

로컬 관리자 계정을 보호하기 위해 관리자가 새 암호를 변경하거나 만들 때 적용되는 암호 복잡성 요구 사항을 정의할 수 있습니다. 개별 계정에 적용할 수 있는 암호 프로파일과 달리 암호 복잡성 규칙은 방화벽 전체에 적용되며 모든 암호에 적용됩니다.

정기적인 비밀번호 업데이트를 시행하려면 비밀번호의 유효 기간을 정의하는 비밀번호 프로파일을 만드십시오.

STEP 1 | 최소 암호 복잡성 설정을 구성합니다.

1. **Panorama** > 설정 > 관리를 선택하고 최소 암호 복잡성 섹션을 편집합니다.
2. 활성화를 선택합니다.
3. 암호 형식 요구 사항을 정의합니다. 암호에 포함해야 하는 대문자, 소문자, 숫자 및 특수 문자에 대한 요구 사항을 적용할 수 있습니다.
4. 계정 사용자 이름(또는 이름의 역버전)이 암호에 사용되지 않도록 하려면 사용자 이름 포함 차단(역방향 포함)을 선택합니다.
5. 암호 기능 요구 사항을 정의합니다.

   관리자에 대한 암호 프로파일을 구성한 경우 암호 프로파일에 정의된 값이 이 섹션에서 정의한 값보다 우선합니다.

STEP 2 | 암호 프로파일을 생성합니다.

여러 암호 프로파일을 생성하고 보안을 적용하기 위해 필요에 따라 관리자 계정에 적용할 수 있습니다.

1. **Panorama** > 암호 프로파일을 선택하고 추가를 클릭합니다.
2. 암호 프로파일의 이름을 입력하고 다음을 정의합니다.
   1. 필수 비밀번호 변경 기간 - 비밀번호를 변경해야 하는 빈도(일).
   2. 만료 경고 기간 - 관리자가 암호 미리 알림을 받을 만료 전의 기간(일 단위)입니다.
   3. 사후 만료 유예 기간 - 관리자가 암호가 만료된 후에도 시스템에 로그인할 수 있는 기간(일 단위)입니다.
   4. 사후 만료 관리자 로그인 횟수 - 암호가 만료된 후 관리자가 시스템에 로그인할 수 있는 횟수입니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 플러그인

Panorama 확장 가능한 플러그인 아키텍처는 VMware NSX와 같은 타사 통합 플러그인과 GlobalProtect 클라우드 서비스와 같은 기타 Palo Alto Networks 제품을 지원합니다. 이 모듈식 아키텍처를 사용하면 새로운 PAN-OS 버전을 기다리지 않고도 새로운 기능을 활용할 수 있습니다.

Panorama에서 VM 시리즈 플러그인을 구성할 수도 있습니다. VM-Series 플러그인은 GCP(Google Cloud Platform), Azure, AWS와 같은 퍼블릭 클라우드 환경과 KVM, ESXi 등과 같은 프라이빗 클라우드 하이퍼바이저와 통합할 수 있는 단일 플러그인입니다. VM-Series 플러그인을 사용하면 공용 클라우드에 배포된 VM-Series 방화벽에서 메트릭을 퍼블리싱할 수 있습니다. Panorama를 사용하여 공용 클라우드에 대한 VM 시리즈 플러그인 설정을 구성하고 구성을 관리형 방화벽에 푸시할 수 있습니다.

- Panorama 플러그인 정보
- VM 시리즈 플러그인 및 Panorama 플러그인
- Cisco TrustSec에 대한 엔드포인트 모니터링

Panorama 플러그인 정보

Panorama는 다음 기능의 통합 및 구성을 가능하게 하는 확장 가능한 플러그인 아키텍처를 지원합니다.

- **AIOps** - Panorama용 AIOps 플러그인을 사용하면 커밋을 검증하고 Panorama로 푸시하기 전에 정책 이 작업이 필요한지 알려줌으로써 모범 사례 검사를 사전에 적용할 수 있습니다.
- **AWS** - AWS 플러그인을 사용하면 AWS에서 EC2 워크로드를 모니터링할 수 있습니다. 플러그인을 사용하면 Panorama(PAN-OS 8.1.3 버전 이상)와 AWS VPC 간의 통신을 활성화하여 Panorama가 사전 정의된 속성 세트(또는 메타데이터 요소)를 EC2 인스턴스에 대한 태그로 수집하고 등록할 수 있습니다. Palo Alto Networks 방화벽에 정보를 제공합니다. 동적 주소 그룹에서 이러한 태그를 참조하고 보안 정책 규칙에서 태그와 일치시키면 VPC 내에 배포된 모든 자산에 일관되게 정책을 시행할 수 있습니다.
- **Azure** - Azure 플러그인을 사용하면 Azure 퍼블릭 클라우드에서 가상 머신을 모니터링할 수 있습니다. 플러그인을 사용하면 Panorama(PAN-OS 8.1.6 버전 이상)와 Azure 구독 간의 통신을 활성화할 수 있으며 Panorama가 Azure 가상 머신의 태그처럼 사전 정의된 속성(또는 메타데이터 요소) 집합을 수집할 수 있고 Palo Alto Networks 방화벽에 정보를 등록할 수 있습니다. 동적 주소 그룹에서 이러한 태그를 참조하고 보안 정책 규칙에서 해당 태그와 일치시키면 구독의 VNet 내에 배포된 모든 자산에 일관되게 정책을 적용할 수 있습니다.
- **Cisco ACI** - Cisco ACI 플러그인을 사용하면 Cisco ACI 패브릭에서 엔드포인트를 모니터링할 수 있습니다. 플러그인을 사용하여 Panorama(8.1.6 버전 이상)와 Cisco APIC 간의 통신을 활성화하면 Panorama가 엔드포인트 정보를 엔드포인트 그룹에 대한 태그로 수집하고 정보를 Palo Alto Networks 방화벽에 등록할 수 있습니다. 동적 주소 그룹에서 이러한 태그를 참조하고 보안 정책 규칙에서 해당 태그와 일치시키면 Cisco ACI 패브릭 내에 배치된 모든 자산에 일관되게 정책을 시행할 수 있습니다.
- **Cisco TrustSec** - Cisco TrustSec 플러그인을 사용하면 Cisco TrustSec 환경에서 엔드포인트를 모니터링할 수 있습니다. 플러그인을 사용하여 Panorama와 Cisco pxGrid 서버 간의 통신을 활성화하면 Panorama가 엔드포인트 정보를 엔드포인트에 대한 태그로 수집하고 정보를 Palo Alto Networks 방화벽에 등록할 수 있습니다. 동적 주소 그룹에서 이러한 태그를 참조하고 보안 정책 규칙에서 해당 태그와 일치시키면 Cisco TrustSec 환경 내에 배치된 모든 자산에 일관되게 정책을 시행할 수 있습니다.
- 클라우드 서비스 — 클라우드 서비스 플러그인을 사용하면 Strata Logging Service와 Prisma Access를 사용할 수 있습니다. Strata Logging Service는 운영 로깅 문제를 해결하고 Prisma Access 클라우드 서비스는 보안 인프라를 원격 네트워크 위치 및 모바일 인력으로 확장합니다.
- 엔터프라이즈 **DLP**(데이터 손실 방지) - 엔터프라이즈 DLP는 무단 액세스, 오용, 추출 또는 공유로부터 민감한 정보를 보호할 수 있는 도구 및 프로세스 세트입니다. Enterprise DLP는 클라우드 서비스를 통해 활성화되어 콘텐츠를 검사하고 올바른 컨텍스트에서 데이터를 분석하여 민감한 데이터를 정확하게 식별하고 사고를 방지하기 위해 보호할 수 있습니다. Enterprise DLP는 PAN-OS 10.0.2 이상의 버전을 실행하는 Panorama 및 관리 방화벽에서 지원됩니다.
- **GCP** - Google Kubernetes Engine(GKE) 클러스터에서 Kubernetes 서비스를 보호할 수 있습니다. Google Cloud Platform(GCP)용 Panorama 플러그인을 구성하여 GKE 클러스터에 연결하고 인터넷에 노출되는 서비스에 대해 알아보세요.
- **Panorama Interconnect** - Panorama Interconnect 플러그인을 사용하면 대규모 방화벽 배포를 관리할 수 있습니다. Interconnect 플러그인을 사용하여 수평 확장 아키텍처에 대한 2계층 Panorama 배포(PAN-OS 8.1.3 버전 이상의 Panorama)를 설정합니다. Interconnect 플러그인을 사용하면 최대

 ©2024 Palo Alto Networks, Inc.

64개의 Panorama 노드 또는 32개의 Panorama HA 쌍이 있는 Panorama 컨트롤러를 배포하여 다수의 방화벽을 중앙에서 관리할 수 있습니다.

- **Nutanix** - Nutanix용 Panorama 플러그인은 Nutanix 환경에서 VM 모니터링을 활성화합니다. 이를 통해 Nutanix Prism Central 내에서 가상 머신 인벤토리를 추적할 수 있으므로 Nutanix 환경 내의 변경 사항에 자동으로 적응하는 보안 정책을 일관되게 시행할 수 있습니다. 가상 머신이 프로비저닝, 디프로비저닝 또는 이동될 때 이 솔루션을 사용하면 IP 주소 및 연결된 속성 집합(또는 메타데이터 요소)을 태그로 수집할 수 있습니다. 그런 다음 태그를 사용하여 동적 주소 그룹을 정의하고 보안 정책에서 사용할 수 있습니다. Nutanix용 Panorama 플러그인에는 Panorama 9.0.4 이상의 버전이 필요합니다.
- **SD-WAN** - 소프트웨어 정의 광역 네트워크(SD-WAN) 플러그인을 사용하면 여러 인터넷 및 개인 서비스를 사용하여 지능형 동적 WAN을 생성할 수 있으므로 비용을 절감하고 애플리케이션 품질과 사용성을 극대화할 수 있습니다. 라우터, 방화벽, WAN 경로 컨트롤러 및 WAN 옵티마이저와 같은 구성 요소와 함께 비용이 많이 들고 시간이 많이 소요되는 MPLS를 사용하여 WAN을 인터넷에 연결하는 대신 Palo Alto Networks 방화벽의 SD-WAN을 통해 보다 저렴한 인터넷 서비스 및 간소화된 장비를 사용할 수 있습니다.
- **VMware NSX** - VMware NSX 플러그인을 사용하면 VMware NSX의 VM 시리즈 방화벽을 VMware NSX Manager와 통합할 수 있습니다. 이 통합을 통해 VM 시리즈 방화벽을 ESXi 서버 클러스터에 서비스로 배포할 수 있습니다.
- **VMware vCenter** - VMware vCenter용 Panorama 플러그인을 사용하면 vCenter 환경에서 가상 머신을 모니터링할 수 있습니다. 플러그인은 vCenter 환경에서 가상 머신의 IP 주소를 검색하고 동적 주소 그룹을 사용하여 정책을 구축하는 데 사용할 수 있는 태그로 변환합니다.
- **Zero Touch Provisioning** - ZTP(Zero Touch Provisioning)는 Panorama에 대한 새 방화벽의 온보딩을 단순화하고 자동화하도록 설계되었습니다. ZTP는 네트워크 관리자가 관리되는 방화벽을 지점으로 직접 배송하고 자동으로 Panorama에 방화벽을 추가할 수 있도록 하여 초기 방화벽 배포 프로세스를 간소화하여 기업이 새 방화벽을 배포할 때 시간과 리소스를 절약할 수 있도록 합니다. ZTP는 PAN-OS 9.1.3 이상의 버전에서 지원됩니다.

  FIPS-CC 모드의 *Panorama*에서는 지원되지 않습니다.

- **IPS** 서명 변환기 - Panorama용 IPS 서명 변환기 플러그인은 타사 침입 방지 시스템(Snort 및 Suricata)의 규칙을 맞춤형 Palo Alto Networks 위협 서명으로 변환하는 자동화된 솔루션을 제공합니다. 그런 다음 지정한 디바이스 그룹에 속한 방화벽에 해당 서명을 등록하고 이를 사용하여 취약점 보호 및 안티-스파이웨어 보안 프로파일에서 정책을 시행할 수 있습니다.

여러 플러그인을 설치하고 단일 Panorama 인스턴스의 여러 소스에서 IP 주소 업데이트를 검색할 수 있습니다. 이를 통해 여러 클라우드 환경에서 애플리케이션과 워크로드를 보호하기 위해 일관된 보안 정책을 생성하고 시행할 수 있습니다. 검색된 IP 주소는 동적 주소 그룹을 통해 보안 정책에 사용됩니다. 작업 부하가 환경에서 추가되거나 제거되면 Panorama는 변경 사항을 등록하고 업데이트를 방화벽에 반영합니다. Panorama에 여러 플러그인을 배포할 때 업데이트가 방화벽에 올바르게 전달되도록 디바이스 그룹 계층 구조를 신중하게 계획해야 합니다.

다양한 플러그인 버전 및 호환성 정보에 대한 자세한 내용은 Palo Alto Networks 호환성 매트릭스를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

Panorama 플러그인 설치

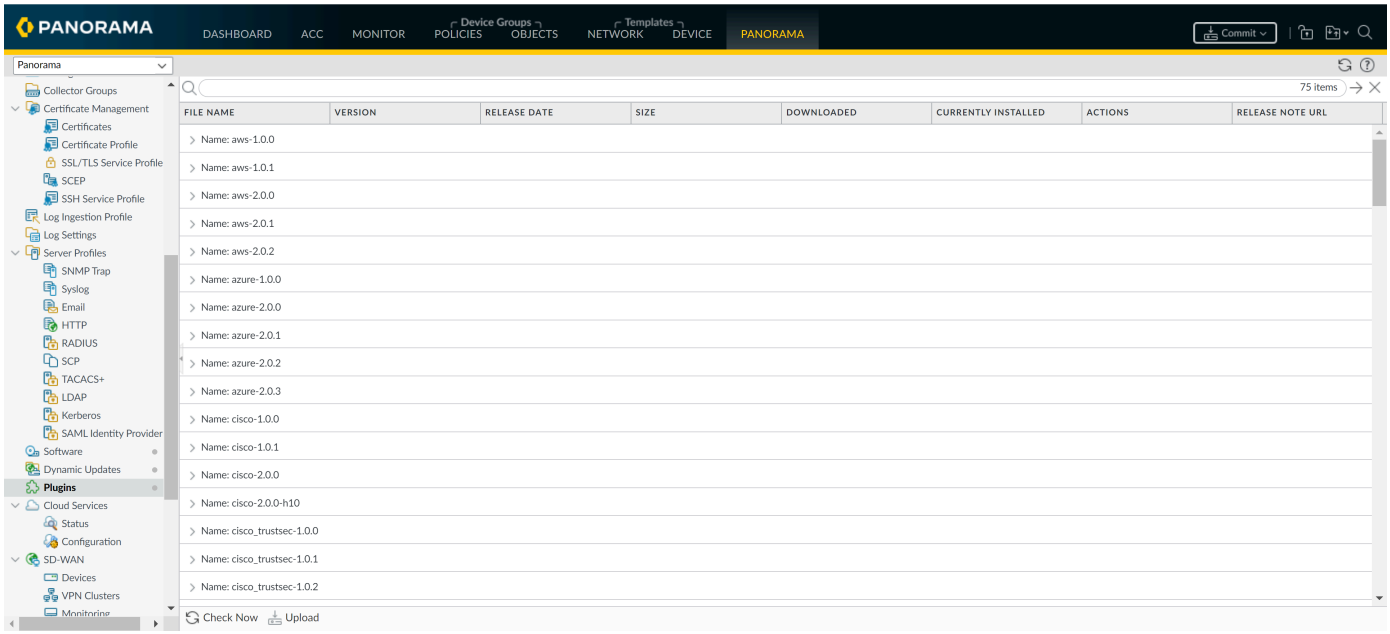
Panorama에 사용 가능한 플러그인 중 하나 이상을 설치하여 클라우드 서비스, VMware NSX를 통합하거나 AWS 또는 Azure 퍼블릭 클라우드에서 가상 머신을 모니터링할 수 있습니다.

클라우드 서비스 플러그인의 경우 고객 지원 포털에서 유효한 인증 코드를 활성화하고 로그를 보낼 지역(미주 또는 유럽)을 선택해야 합니다.

현재 설치된 플러그인 버전이 있고 새 버전의 플러그인을 설치하면 *Panorama*가 현재 설치된 버전을 대체합니다.

STEP 1 | 플러그인을 다운로드합니다.

1. **Panorama** > 플러그인을 선택합니다.



2. 지금 확인을 선택하여 사용 가능한 업데이트 목록을 검색합니다.
3. 작업 열에서 다운로드를 선택하여 플러그인을 다운로드합니다.

   각 Panorama 플러그인에 대해 지원되는 최소 PAN-OS 버전은 호환성 매트릭스를 참조하십시오.

STEP 2 | 플러그인을 설치합니다.

플러그인 버전을 선택한 다음 작업 열에서 설치를 클릭하여 플러그인을 설치합니다. 설치가 완료되면 Panorama가 알려줍니다. 플러그인 설치에 대한 자세한 내용은 VMware NSX 플러그인 또는 클라우드 서비스 플러그인 설명서를 참조하십시오.

Panorama HA 쌍에 플러그인을 처음 설치할 때 활성 피어보다 먼저 수동 피어에 플러그인을 설치하십시오. 패시브 피어에 플러그인을 설치하면 비기능 상태로 전환됩니다. 그런 다음 활성 피어에 플러그인을 성공적으로 설치한 후 수동 피어가 기능 상태로 돌아갑니다.

©2024 Palo Alto Networks, Inc.

VM 시리즈 플러그인 및 Panorama 플러그인

VM 시리즈 플러그인과 Panorama용 다양한 플러그인의 차이점은 무엇입니까?

VM-Series Plugin은 VM-Series 방화벽용으로 GCP(Google Cloud Platform), Azure, AWS 등의 퍼블릭 클라우드 환경과 KVM, ESXi 등의 프라이빗 클라우드 하이퍼바이저와 통합할 수 있는 단일 플러그인입니다. 방화벽을 배포할 때 기본 제공 플러그인은 방화벽이 배포된 가상 환경을 자동으로 감지하고 해당 클라우드 환경과의 상호 작용을 관리할 수 있는 플러그인 구성 요소를 로드합니다. 예를 들어 VM 시리즈 방화벽을 GCP에 배포하면 VM 시리즈 방화벽은 GCP와의 통합을 가능하게 하는 플러그인 구성요소를 로드합니다. 그런 다음 VM 시리즈 플러그인을 사용하여 Google Stackdriver Monitoring에 측정 항목을 게시하도록 GCP의 VM 시리즈 방화벽을 구성할 수 있습니다. 마찬가지로 Azure의 VM 시리즈 방화벽에 있는 VM 시리즈 플러그인을 사용하면 Azure Application Insights 메트릭을 게시하도록 방화벽을 구성하거나 방화벽이 HA 쌍으로 작동하는 데 필요한 세부 정보를 설정할 수 있습니다. VM-Series 플러그인은 VM-Series 방화벽에 사전 설치되어 있으며 업그레이드 또는 다운그레이드할 수 있지만 삭제할 수는 없습니다. Panorama에서 VM-Series 플러그인을 사용할 수 있지만 사전 설치되어 있지는 않습니다. Panorama를 사용하여 방화벽의 통합을 관리하기로 선택한 경우 Panorama에 VM-Series 플러그인을 설치하여 방화벽의 VM-Series 플러그인과 통신을 설정하십시오.

Panorama 플러그인은 하드웨어 기반 방화벽과 VM 시리즈 방화벽 모두에 적합합니다. Panorama 플러그인은 선택 사항이므로 Panorama에서 추가, 제거, 재설치 또는 업그레이드할 수 있습니다. Panorama 플러그인은 내장되어 있지 않으며, 필요한 관리 환경과 통신이 가능하도록 플러그인을 설치해야 합니다. 예를 들어, Panorama에서 Cloud Services 플러그인을 사용하여 Panorama/방화벽과 Cortex Data Lake 간의 설정을 활성화합니다. Panorama의 GCP 플러그인을 사용하면 Panorama와 GCP 배포 간의 통신이 가능하므로 Google Kubernetes Engine(GKE) 클러스터에 배포된 서비스에 들어오거나 나가는 트래픽을 보호할 수 있습니다.

Panorama에 VM 시리즈 플러그인 설치

VM 시리즈 방화벽에 배포된 클라우드 통합을 보고 구성하려면 Panorama와 VM 시리즈 방화벽 모두에 VM 시리즈 플러그인을 설치해야 합니다. 플러그인은 방화벽에 자동으로 설치되지만 구성을 디바이스 그룹에 푸시하려면 Panorama에 플러그인을 수동으로 설치해야 합니다.

VM-시리즈 플러그인은 모든 클라우드를 지원하므로 업그레이드가 *VM*-시리즈 방화벽에 적용되지 않을 수 있습니다. 플러그인을 업그레이드하기 전에 버전 정보를 참조하십시오. 클라우드와 관련된 변경 사항이 있는 경우에만 플러그인을 업데이트하십시오.

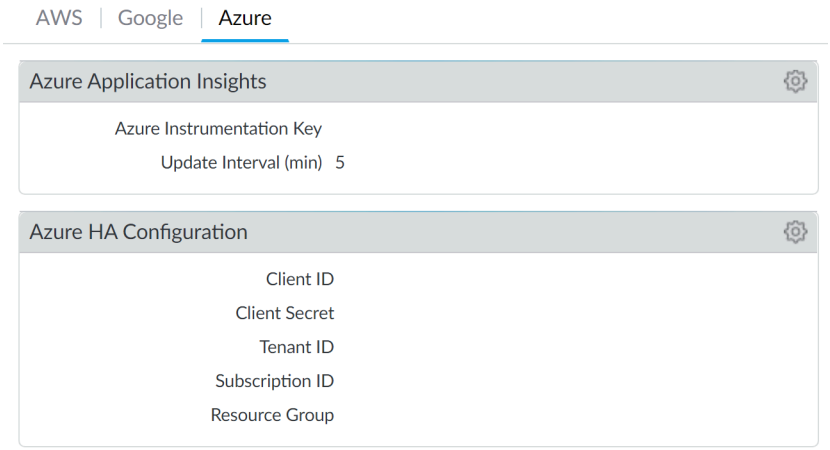
STEP 1 | VM 시리즈 플러그인을 다운로드합니다.

1. **Panorama** > > 플러그인을 선택하고 지금 확인을 사용하여 새 플러그인 패키지를 찾습니다. VM 시리즈 플러그인 이름은 `vm_series`입니다.
2. 어떤 버전이 유용한 업그레이드를 제공하는지 확인하려면 플러그인 버전 정보를 참조하십시오.
3. 플러그인 버전을 선택한 다음 작업 열에서 다운로드를 선택합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | VM 시리즈 플러그인을 설치합니다.

1. 작업 열에서 설치를 클릭합니다. 설치가 완료되면 Panorama가 알려줍니다.
2. 플러그인을 보려면 디바이스 > **VM-Series**를 선택합니다.
   - 방화벽이 사설 클라우드에 설치되어 있고 하이퍼바이저 또는 서비스에 통합이 없는 경우, 하이퍼바이저가 출시한 새로운 기능 또는 새로운 보안 요구 사항을 충족하기 위해 VM-Series라는 탭과 기본 메시지인 `VM Series #### ### ### #### ## ## #### ### ## # # ####.`
   - 방화벽이 공용 클라우드에 배포된 경우 Panorama는 지원되는 모든 클라우드에 대한 탭을 표시합니다.



STEP 3 | (선택 사항) 구성을 저장하고 관리형 방화벽에 푸시합니다.

STEP 4 | (선택 사항) VM 시리즈 방화벽에서 디바이스 > **VM** 시리즈를 선택합니다. 플랫폼에 대한 통합을 구성한 경우 방화벽이 배포된 클라우드에 대한 단일 탭이 표시됩니다. 통합을 구성하지 않은 경우 VM 시리즈 플러그인 인프라에 대한 기본 메시지가 표시됩니다.

©2024 Palo Alto Networks, Inc.

Cisco TrustSec에 대한 엔드포인트 모니터링

Cisco TrustSec용 Panorama 플러그인을 설치 및 구성하여 사용자 환경에서 엔드포인트의 IP 주소를 검색하고 동적 주소 그룹을 사용하여 해당 엔드포인트에 대한 보안 정책을 구축합니다.

- Cisco TrustSec용 Panorama 플러그인
- Cisco TrustSec용 Panorama 플러그인 설치
- Cisco TrustSec용 Panorama 플러그인 구성
- Cisco TrustSec용 Panorama 플러그인 문제 해결

Cisco TrustSec용 Panorama 플러그인

Cisco TrustSec용 Panorama 플러그인을 사용하면 동적 또는 정적 주소 그룹을 사용하여 TrustSec 환경에 대한 보안 정책을 생성할 수 있습니다. 플러그인은 TrustSec 보안 그룹의 변경 사항을 모니터링하고 해당 정보를 Panorama에 등록하고 IP 정보를 방화벽에 포워딩하므로 Panorama는 해당 엔드포인트에 올바른 정책을 적용할 수 있습니다. Cisco TrustSec용 Panorama 플러그인은 최대 16개의 pxGrid(Cisco ISE) 서버를 지원합니다.

Panorama 플러그인은 엔드포인트 정보를 처리하고 이를 동적 주소 그룹에 IP 주소를 배치하기 위한 일치 기준으로 사용할 수 있는 태그 세트로 변환합니다. Panorama는 pxGrid 서버의 각 보안 그룹 태그(SGT)에 대한 태그를 생성합니다. 태그는 다음과 같은 형식으로 구성됩니다.

cts.svr_<server-name>.sgt_<SGT-decimal number>

엔드포인트 IP 주소-태그 매핑 정보를 검색하려면 사용자 환경의 각 pxGrid 서버에 대한 모니터링 정의를 구성해야 합니다. pxGrid 서버 구성은 사용자 이름과 암호를 지정하며 Panorama가 pxGrid에 연결할 수 있도록 하는 모니터링 정의에서 참조됩니다. 또한 Panorama에서 인증서 프로파일을 사용하여 pxGrid 서버 ID를 확인하도록 플러그인을 구성할 수 있습니다. Panorama가 태그를 푸시하는 방화벽을 포함하는 디바이스 그룹과 해당 알림 그룹도 지정합니다. 모니터링 정의를 구성하고 플러그인이 태그를 검색한 후 동적 주소 그룹을 생성하고 태그를 일치 기준으로 추가할 수 있습니다.

Cisco TrustSec용 Panorama 플러그인 버전 1.0.2 이상은 대량 동기화 및 PubSub 모니터링 모드를 지원합니다. 플러그인은 Panorama 버전을 기반으로 모드를 선택합니다. 즉, Panorama 10.0.0 이전 버전이면 대량 동기화 모드를 선택하고 Panorama 10.0.0 이상이면 PubSub 모드를 선택합니다. 사용자 인터페이스에는 기본 모니터링 모드의 구성 옵션이 표시됩니다.

- 대량 동기화
- PubSub

대량 동기화

대량 동기화 모드는 pxGrid 서버에서 정보를 검색하기 위해 모니터링 간격과 전체 동기화 간격이라는 두 가지 간격을 사용합니다. Cisco TrustSec용 Panorama 플러그인 버전 1.0.2 이상이 Panorama 10.0.0 이전 버전에 설치된 경우 이 모드가 기본값입니다. 10.0.0 이전의 Panorama 버전은 10초마다 구성된 IP-탭 업데이트를 지원합니다.

- 모니터링 간격 — 모니터링 간격은 플러그인이 변경 사항을 쿼리하기 전에 대기하는 시간입니다. 변경 사항이 없는 경우 모니터링 간격이 재설정됩니다. 변경 사항이 있는 경우 플러그인은 변경 사항을 먼

 ©2024 Palo Alto Networks, Inc.

저 처리한 후에 모니터링 간격을 재설정합니다. 기본 모니터링 간격은 60초입니다. 모니터링 간격은 10초~하루(86,400초) 범위로 설정할 수 있습니다.

*Cisco TrustSec*용 *Panorama* 플러그인 *1.0.0*이 설치된 경우 최소 모니터링 간격은 *30*초입니다.

- 전체 동기화 간격 — 전체 동기화 간격은 변경 사항에 관계없이 플러그인이 모든 pxGrid 서버에서 동적 개체를 업데이트하기 전에 대기하는 시간입니다. 이렇게 하면 모니터링 간격에 따라 변경 이벤트를 놓친 경우에도 플러그인이 pxGrid 서버와 동기화됩니다. 전체 동기화 간격은 600초(10분)~86,400초(하루) 범위로 설정할 수 있습니다. Panorama CLI에서 전체 동기화 간격을 구성해야 합니다.

모니터링 간격이 전체 동기화 간격보다 클 경우 전체 동기화 간격이 무시되고 모든 모니터링 간격마다 전체 동기화가 수행됩니다.

PubSub

PubSub 모드는 Cisco ISE 서버(구독 데몬)에서 직접 알림을 모니터링하고, IP 태그를 구문 분석하고, 관련 정보를 태그 처리 데몬(tag-proc)에 보냅니다. Cisco TrustSec용 Panorama 플러그인 버전 1.0.2 이상이 Panorama 10.0.0 이상 버전에 설치된 경우 PubSub이 기본 모드입니다. Panorama 버전 10.0.0 이상에서는 100밀리초마다 구성된 IP-탭 업데이트를 지원합니다.

- 푸시 간격 — 푸시 간격은 푸시 사이의 시간입니다. 이전 푸시에 시간이 너무 오래 걸리면 완료되는 즉시 다음 푸시가 트리거됩니다. 최소 푸시 간격은 100밀리초(0초)이고 최대 푸시 간격은 60초입니다. 기본 푸시 간격은 0초입니다.
- 전체 동기화 활성화 — 전체 업데이트를 트리거하려면 이 옵션을 활성화합니다. 전체 동기화를 활성화한 경우 전체 동기화 간격을 설정할 수 있습니다. 기본값은 아니요입니다.
- 전체 동기화 간격 — 전체 동기화 간격은 변경 사항에 관계없이 플러그인이 모든 pxGrid 서버에서 동적 개체를 업데이트하기 전에 대기하는 시간입니다. 기본 전체 동기화 간격은 10분입니다. 전체 동기화 간격은 600초(10분)~86,400초(하루) 범위로 설정할 수 있습니다. Panorama CLI에서 전체 동기화 간격을 구성해야 합니다.
- 재연결 간격 — 초기 재연결 간격은 1초이며, 이전 재연결에 실패한 경우 두 배로 늘어납니다. 최대 재연결 간격은 64초이며 재연결 시도 횟수에는 제한이 없습니다.

동적 주소와 정적 주소 간의 차이점

Cisco TrustSec용 Panorama 플러그인을 사용하여 동적 또는 정적 주소 그룹으로 보안 정책을 생성할 수 있습니다. Cisco ISE 서버에서 수신한 매핑은 Panorama 플러그인 프레임워크에서 처리되기 전에 변환됩니다. 사용자 지정 태그를 나타내는 이 변환은 pxGrid 서버 이름과 수신한 SGT를 기반으로 합니다.

```
cts.svr_<server-name>.sgt_<SGT-decimal number>
```

SGT 이름은 Cisco ISE 서버에서 다음과 같은 세 가지 형식으로 표시됩니다.

- 문자열 — 예: BYOD
- 십진수 — 예: 15
- **16**진수 — 예: 000F

SGT 이름의 형식은 SGT 유형에 따라 달라집니다.

©2024 Palo Alto Networks, Inc.

- 동적 SGT에서 사용하는 **com.cisco.ise.session service**는 태그를 문자열 형식으로 반환합니다. 이 형식을 사용하면 일치 기준을 다음과 같이 구성할 수 있습니다.

  ```
  cts.svr_<server-name>.sgt_BYOD
  ```

- 정적 SGT에서 사용하는 **com.cisco.ise.sxp service**는 태그를 십진수 형식으로 반환합니다. 따라서 정적 SGT의 일치 기준은 다음과 같습니다.

  ```
  cts.svr_<server-name>.sgt_15
  ```

동일한 주소 그룹에 동적 SGT와 정적 SGT를 모두 포함할 수 있지만 일치 기준에는 두 형식이 모두 포함되어야 합니다.

```
cts.svr_<server-name>.sgt_BYOD
```

또는

```
cts.svr_<server-name>.sgt.15
```

Cisco TrustSec용 Panorama 플러그인 설치

Panorama에서 Cisco TrustSec 플러그인을 다운로드하고 설치하여 Cisco TrustSec으로 엔드포인트 모니터링을 시작합니다. 플러그인 버전과 Panorama 버전을 연관시키려면 호환성 매트릭스의 Panorama 플러그인을 참조하십시오.

Cisco TrustSec 플러그인 업그레이드 또는 다운그레이드에는 커밋이 필요합니다.

Panorama HA 구성이 있는 경우 각 Panorama 피어에서 이 설치 과정을 반복합니다. HA 쌍의 Panorama 어플라이언스에 플러그인을 처음 설치할 경우 액티브 피어보다 먼저 패시브 피어에 플러그인을 설치합니다. 패시브 피어에 플러그인을 설치하면 비작동 상태로 전환됩니다. 액티브 피어에 플러그인을 설치하면 패시브 피어가 작동 상태로 돌아갑니다.

HA 쌍에 설치된 독립형 Panorama 또는 두 개의 Panorama 어플라이언스에 여러 플러그인이 설치된 경우, 플러그인 중 하나 이상이 구성되지 않으면 업데이트된 IP 태그 정보를 수신하지 못할 수 있습니다. 이는 Panorama가 IP 태그 정보를 구성되지 않은 플러그인으로 포워딩하지 않기 때문입니다. 또한 Panorama 플러그인 중 하나 이상이 등록됨 또는 성공 상태가 아닐 경우 이 문제가 발생할 수 있습니다(긍정 상태는 플러그인마다 다름). 아래 설명된 명령을 진행하거나 실행하기 전에 플러그인이 긍정 상태인지 확인합니다.

이 문제가 발생하면 두 가지 해결 방법이 있습니다.

- 구성되지 않은 플러그인 또는 플러그인을 제거합니다. 바로 구성하지 않을 플러그인은 설치하지 않는 것이 좋습니다.

 ©2024 Palo Alto Networks, Inc.

- 다음 명령을 사용하여 이 문제를 해결할 수 있습니다. 각 Panorama 인스턴스에서 구성되지 않은 각 플러그인에 대해 다음 명령을 실행하여 Panorama가 업데이트를 보내기 위해 기다리지 않도록 해야 합니다. 그렇지 않으면 방화벽이 일부 IP 태그 정보를 잃을 수 있습니다.

  request plugins dau plugin-name <plugin-name> unblock-device-push yes

  다음을 실행하여 이 명령을 취소할 수 있습니다.

  request plugins dau plugin-name <plugin-name> unblock-device-push no

설명된 명령은 재부팅에 영구적으로 적용되는 것은 아니며 이후에 재부팅할 경우 다시 사용해야 합니다. HA 쌍의 Panorama는 각 Panorama에서 명령을 실행해야 합니다.

STEP 1 | **Panorama** > 플러그인을 선택합니다.

STEP 2 | 플러그인의 최신 버전을 다운로드하려면 지금 확인을 클릭합니다.

STEP 3 | 작업 열에서 다운로드를 선택하여 플러그인을 다운로드합니다.

STEP 4 | 플러그인 버전을 선택한 다음 작업 열에서 설치를 클릭하여 플러그인을 설치합니다. 설치가 완료되면 Panorama가 알려줍니다.

Cisco TrustSec용 Panorama 플러그인 구성

플러그인을 설치한 후에는 Cisco TrustSec 플러그인 구성에 알림 그룹도 할당해야 합니다. 알림 그룹은 Panorama가 pxGrid 서버에서 검색한 모든 태그를 푸시해야 하는 방화벽을 포함하는 디바이스 그룹 목록입니다.

Cisco TrustSec 플러그인이 설치된 각 Panorama는 최대 16개의 pxGrid 서버와 16개의 모니터링 정의를 지원할 수 있습니다. 그리고 각 모니터링 정의에는 하나의 pxGrid 서버와 하나의 알림 그룹이 있습니다.

다음 구성 지침은 대량 동기화 및 PubSub 모니터링 모드 모두에 적용되며 모니터링 모드에 따라 일부 사용자 인터페이스 기능이 활성화되거나 표시됩니다.

STEP 1 | 전체 동기화 간격을 기본값인 600초(10분)에서 변경하려면 전체 동기화 간격을 구성합니다.

1. Panorama CLI에 로그인합니다.
2. 구성 모드로 전환합니다.

   admin@Panorama> configure
3. 다음 명령을 사용하여 전체 동기화 간격을 설정합니다. 범위는 600초~86,400초(하루)입니다.

   admin@Panorama# set plugins cisco_trustsec full-sync-interval <interval-in-seconds>

STEP 2 | Panorama 웹 인터페이스에 로그인합니다.

STEP 3 | Panorama에서 방화벽을 관리되는 디바이스로 추가하고 디바이스 그룹을 생성해야 Panorama가 검색한 VM 정보를 해당 그룹에 알리도록 구성할 수 있습니다. 디바이스 그룹에는 VM-Series 방화벽이나 하드웨어 방화벽의 가상 시스템이 포함될 수 있습니다.

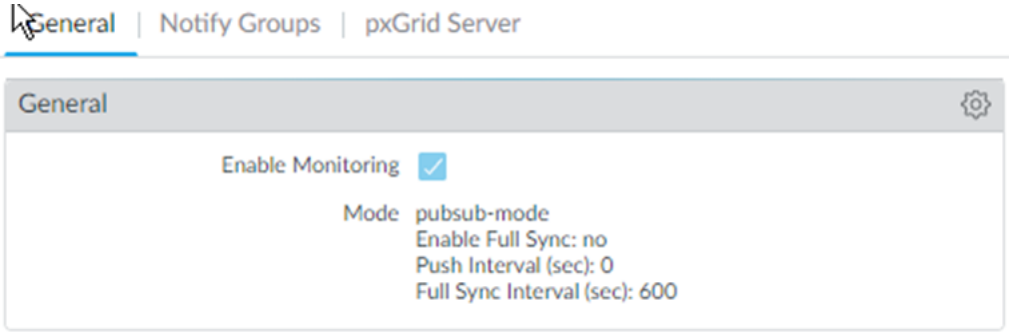
 ©2024 Palo Alto Networks, Inc.

STEP 4 | Cisco TrustSec 모니터링을 구성합니다.

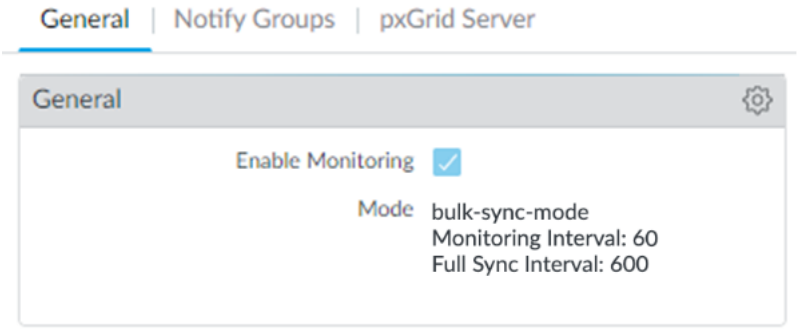
1. **Panorama** > **Cisco TrustSec** > 설정 > 일반을 선택합니다.

   기본적으로 **Cisco TrustSec** 모니터링 사용이 활성화되어 있습니다. 이를 통해 배포 내 모든 클러스터를 모니터링할 수 있습니다.

   Cisco TrustSec용 Panorama 플러그인이 1.0.2 이상이고 Panorama 10.0.0 이상에 설치된 경우 사용자 인터페이스는 PubSub 모니터링 모드를 선택합니다.

   플러그인이 Panorama 10.0.0 이전 버전에 설치된 경우 대량 동기화 모드를 선택합니다.

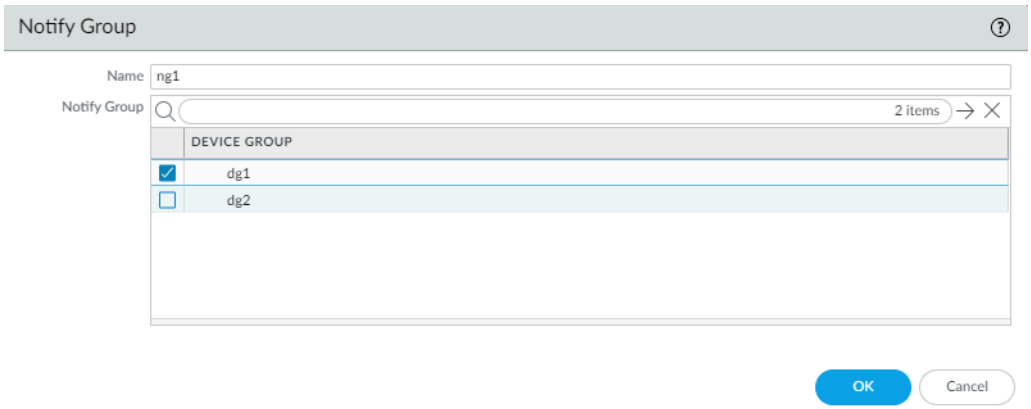
   

2. 기어를 클릭하여 설정 매개변수를 편집합니다.
   - 푸시 간격(PubSub만 해당) — 최소값은 0이고, 최대값은 60초이며, 기본값은 0(100밀리초)입니다.
   - 전체 동기화 사용(PubSub만 해당, 선택 사항) — 이 옵션을 선택하면 전체 동기화가 활성화됩니다. 기본값은 아니요입니다.
   - 전체 동기화 간격
     - PubSub — 전체 동기화 사용을 선택한 경우 전체 동기화 간격을 초 단위로 설정할 수 있습니다. 범위는 600초~86,400초(하루)이며 기본값은 600입니다.
     - 대량 동기화 — 대량 동기화 모드에서는 기본적으로 이 옵션이 활성화됩니다. 범위는 600초~86,400초(하루)이며 기본값은 600입니다.
   - 모니터링 간격(대량 동기화만 해당) — 범위는 10초~86,400초이며 기본값은 60입니다. Panorama가 pxGrid 서버에 엔드포인트 주소 정보를 쿼리하는 폴링 간격을 설정합니다. 모니터링 이벤트 종료 시간과 다음 이벤트 시작 시간 사이의 기간입니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 알림 그룹을 생성합니다.

1. **Panorama** > **Cisco TrustSec** > 설정 > 알림 그룹을 선택합니다.
2. 추가를 클릭합니다.
3. 알림 그룹을 설명하는 이름을 입력합니다.
4. 이전에 생성한 디바이스 그룹을 선택합니다.



STEP 6 | (선택 사항) pxGrid 서버의 서버 ID 확인을 활성화하는 경우 Panorama에서 인증서 프로파일을 구성합니다.

STEP 7 | pxGrid 클라이언트 이름 및 클라이언트 암호를 생성, 활성화 및 승인합니다.

1. Panorama CLI에 로그인합니다.
2. 다음 명령을 실행하여 클라이언트 이름을 생성합니다.
   - 인증서 프로파일이 있는 경우 다음과 같이 클라이언트 이름을 생성합니다.

     admin@Panorama> request plugins cisco_trustsec create-account client-name <client-name> host <ise-server-ip>
   - 6단계를 건너뛰었고 인증서가 없는 경우 다음을 입력합니다.

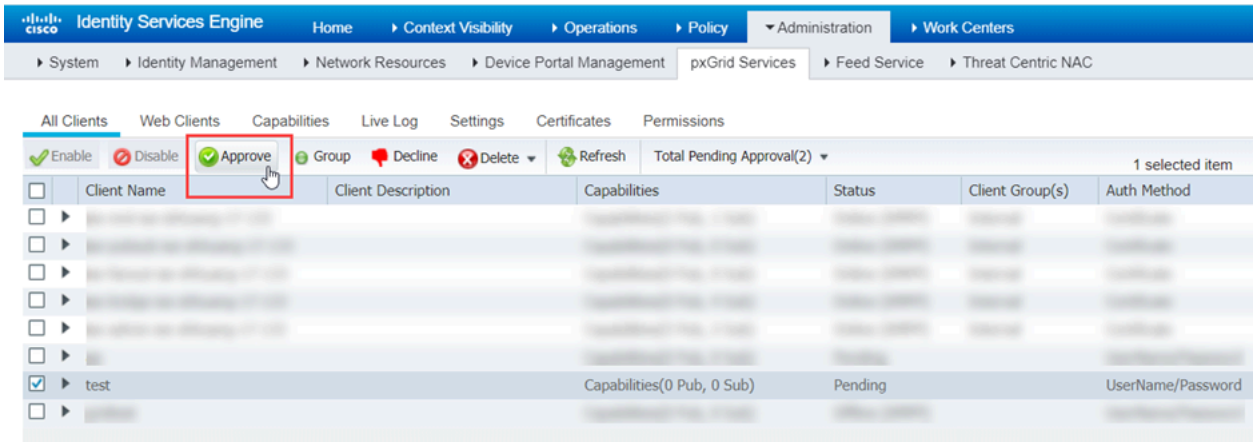
     request plugins cisco_trustsec create-account server-cert-verification-enabled no client-name <client-name>host <host-name>
3. 다음 명령을 실행하여 클라이언트 이름을 생성합니다.

```
admin@Panorama> request plugins cisco_trustsec create-account
 client-name test host 10.10.10.15 AccountCreate ## #...
```


©2024 Palo Alto Networks, Inc.

```
AccountCreate ##.   ##### ## ##: test ##### ##: <xxxxxxxx>
AccountActivate ## #... AccountActivate ##. #### ### ######.
```

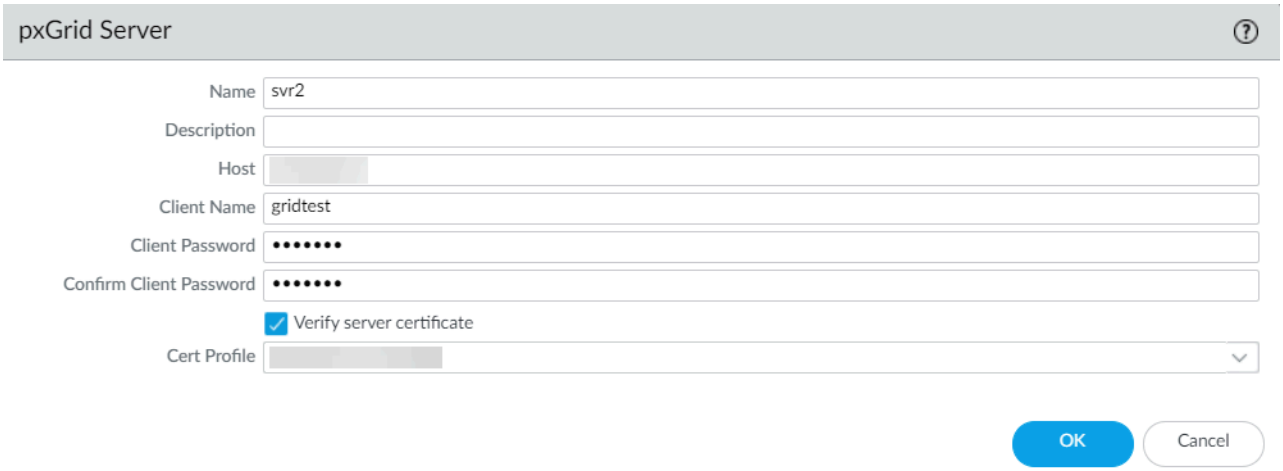
4. Cisco ISE 서버에 로그인하여 계정을 승인합니다.
5. 관리 > **pxGrid** 서비스 > 모든 클라이언트를 선택합니다.
6. Panorama에서 생성한 클라이언트 이름을 선택합니다.
7. 승인을 클릭합니다.



 ©2024 Palo Alto Networks, Inc.

STEP 8 | pxGrid 서버 정보를 추가합니다. Cisco TrustSec용 Panorama 플러그인은 최대 16개의 pxGrid(Cisco ISE) 서버를 지원합니다.

1. **Panorama** > **Cisco TrustSec** > 설정 > **pxGrid** 서버를 선택합니다.
2. pxGrid 서버를 설명하는 이름을 입력합니다.
3. 호스트 필드에 pxGrid 서버의 IP 주소 또는 FQDN을 입력합니다.
4. 이전 단계에서 생성한 클라이언트 이름을 입력합니다.
5. 이전 단계에서 생성한 클라이언트 암호를 입력하고 확인합니다.
6. pxGrid 서버 ID를 확인합니다.
   1. 서버 인증서 확인을 선택합니다.
   2. 인증서 프로파일 드롭다운에서 인증서 프로파일을 선택합니다.
7. 확인을 클릭합니다.



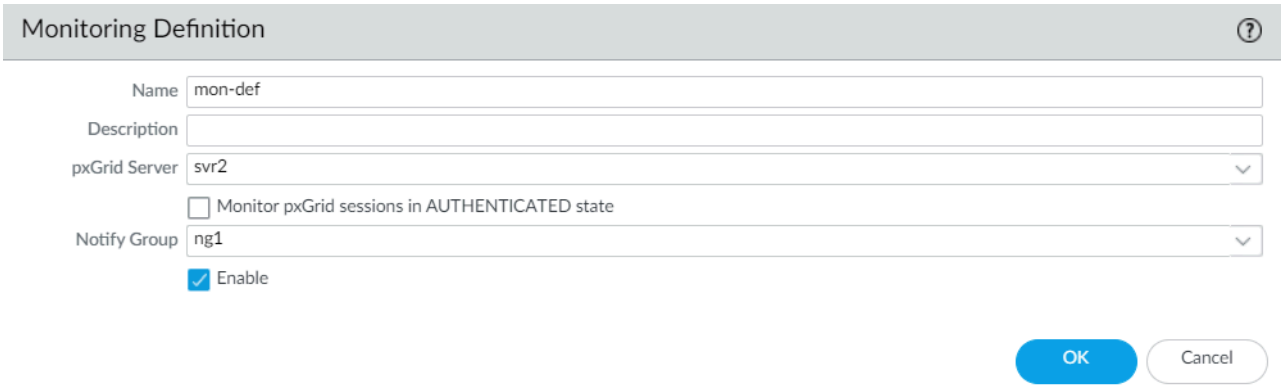
STEP 9 | 모니터링 정의를 구성합니다.

1. **Panorama** > **Cisco TrustSec** > 모니터링 정의를 선택하고 추가를 클릭합니다.
2. 모니터링 정의를 식별할 수 있는 설명이 포함된 이름 및 설명(선택 사항)을 입력합니다.
3. **pxGrid Server**를 선택합니다.
4. (선택 사항) Panorama를 **AUTHENTICATED** 상태에서 **pxGrid** 세션을 모니터링하도록 설정합니다. 기본적으로 Panorama는 “STARTED” 상태의 세션에서 IP 태그 매핑을 검색합니다. 해당

 ©2024 Palo Alto Networks, Inc.

하는 계정 시작 패킷이 있는 경우 ISE 세션은 “STARTED” 상태가 됩니다. 세션에 대한 계정 시작 패킷이 없는 경우 세션 상태는 “AUTHENTICATED”입니다.

5. 알림 그룹을 선택합니다.
6. 확인을 클릭합니다.



STEP 10 | 변경 사항을 커밋합니다.

STEP 11 | Panorama가 동적 또는 정적 주소 그룹 정의를 위한 SGT 태그를 학습할 수 있도록 활성 ISE 세션을 생성합니다. 활성 세션을 생성하려면 ISE를 사용하여 디바이스를 인증합니다.

Panorama는 ISE에서 기본 SGT 태그를 수집하지 않습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 동적 또는 정적 주소 그룹을 생성하고 주소가 추가되었는지 확인합니다.

1. 개체 > 주소 그룹을 선택합니다.
2. 디바이스 그룹 드롭다운에서 Cisco TrustSec 환경의 엔드포인트를 모니터링하기 위해 생성한 디바이스 그룹을 선택합니다.
3. 추가를 클릭하고 주소 그룹에 대한 이름과 설명을 입력합니다.

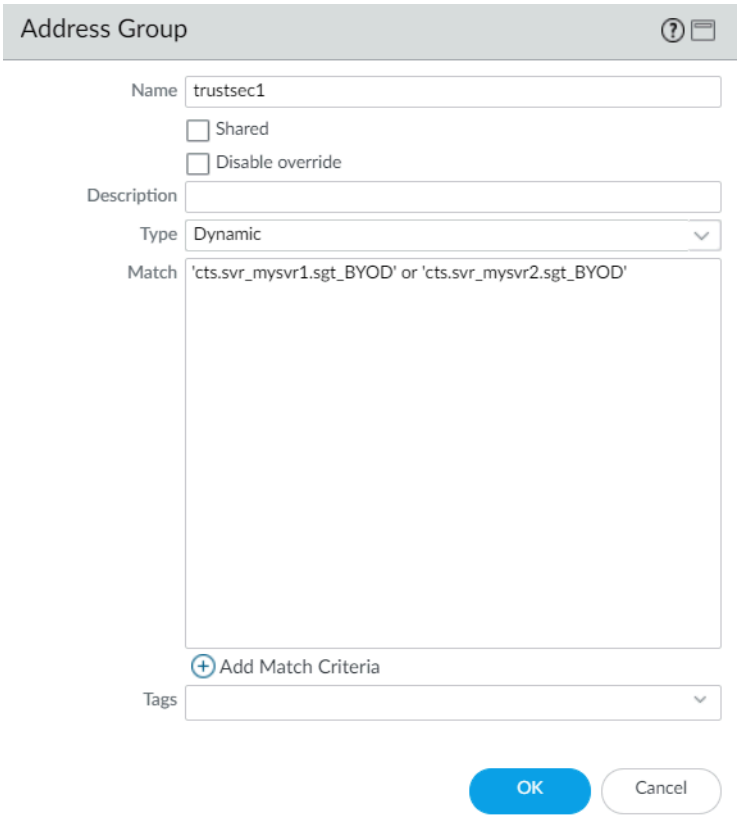
   동적 주소 그룹 명명 규칙: **`cts.svr_<server-name>.sgt_<SGT-name>`**

   정적 그룹 명명 규칙:

   `cts.svr_<server-name>.sgt_<SGT-decimal number>`
4. 유형을 동적 또는 정적으로 선택합니다.
5. 일치 기준 추가를 클릭합니다.
6. **And** 또는 **Or** 연산자를 선택하고 보안 그룹 이름 옆에 있는 더하기(+) 아이콘을 클릭하여 동적 주소 그룹에 추가합니다.

   Panorama는 활성 세션에서 학습한 보안 그룹 태그만 표시할 수 있습니다. 라이브 세션의 보안 그룹 태그가 일치 기준 목록에 표시됩니다.
7. **Panorama** > 개체 > 주소 그룹을 선택합니다.
8. 동적 주소 그룹의 주소 열에서 더 보기를 클릭합니다.

   Panorama는 지정한 일치 기준에 따라 해당 동적 주소 그룹에 추가된 IP 주소 목록을 표시합니다.



 ©2024 Palo Alto Networks, Inc.

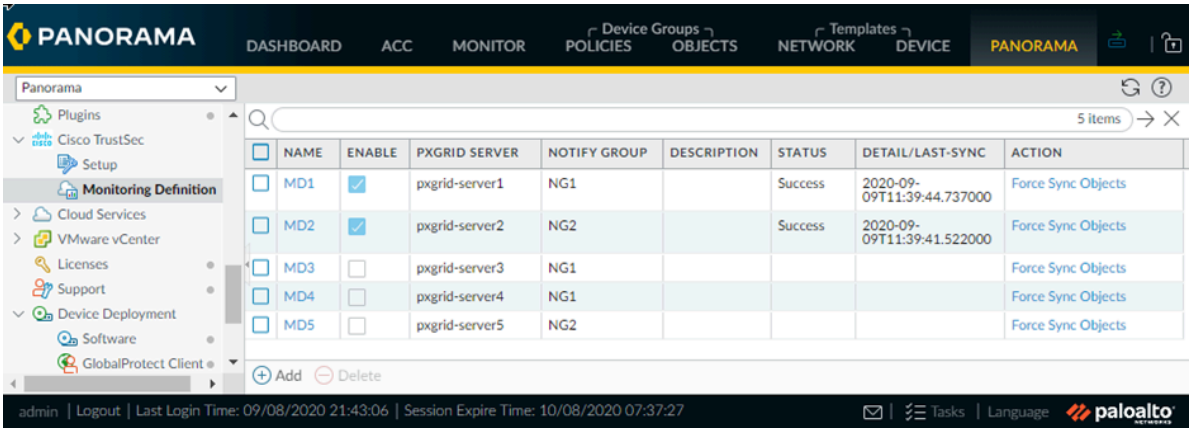
STEP 13 | 정책에 동적 주소 그룹을 사용합니다.

동적 주소 그룹은 정책에 연결할 때까지 비어 있습니다. 정책에서 사용하지 않는 한 동적 주소 그룹에는 *IP* 주소가 표시되지 않습니다.

1. 정책 > 보안을 선택합니다.
2. 추가를 클릭하고 정책에 대한 이름 및 설명을 입력합니다.
3. 소스 영역을 추가하여 트래픽이 시작되는 영역을 지정합니다.
4. 트래픽이 종료되는 대상 영역을 추가합니다.
5. 대상 주소에 대해 방금 생성한 동적 주소 그룹을 선택합니다.
6. 트래픽에 대한 작업(허용 또는 거부)을 지정하고 선택적으로 기본 보안 프로파일을 규칙에 연결합니다.
7. 1단계부터 6단계를 반복하여 다른 정책 규칙을 생성합니다.
8. 커밋을 클릭합니다.

STEP 14 | (선택 사항) 개체를 동기화하여 언제든지 **pxGrid** 서버에서 개체를 업데이트합니다. 개체를 동기화하면 가상 환경의 변경 사항에 대한 컨텍스트를 유지할 수 있으며 정책 규칙에 사용되는 주소 그룹을 자동으로 업데이트하여 애플리케이션을 활성화할 수 있습니다.

1. **Panorama** > **Cisco TrustSec** > 모니터링 정의를 선택합니다.
2. 동적 개체 동기화를 클릭합니다.



Cisco TrustSec용 Panorama 플러그인 문제 해결

- 플러그인 상태 명령
- 디버그 명령
- 디버그 로그

플러그인 상태 명령

- 카운터 지우기:

```
clear plugins cisco_trustsec counters
```


©2024 Palo Alto Networks, Inc.

- 디스플레이 모니터 상태:

```
show plugins cisco_trustsec status
```

- 디스플레이 카운터:

```
show plugins cisco_trustsec counters
```

디버그 명령

- 동적 주소 그룹의 IP 주소를 확인합니다.

```
show object registered-ip tag <tag>
```

```
show object registered-ip all
```

- 서버에서 IP 주소의 태그를 가져옵니다. 가져온 IP 태그 매핑은 `plugin_cisco_trustsec.log`에 기록됩니다. 서버와 연결된 알림 그룹에는 IP 태그 매핑이 푸시되지 않습니다. 실패하면 재시도할 수 없습니다.

```
debug plugins cisco_trustsec query pxgrid-server $server-name ip
 $ip-address
```

- 서버와 강제 동기화하고 매핑을 configd 프로세스로 푸시합니다. 실패하면 재시도할 수 없습니다.

```
request plugins cisco_trustsec synchronize-dynamic-objects name
 $server-name
```

- 모든 서버와 강제 동기화하고 매핑을 configd 프로세스로 푸시합니다. 실패하면 재시도할 수 없습니다.

```
 request plugins cisco_trustsec synchronize-dynamic-objects all
```

- configd 프로세스에서 VM-Series 방화벽으로의 매핑을 강제 동기화합니다. 실패하면 재시도할 수 없습니다.

```
request plugins cisco_trustsec sync
```

디버그 로그

로그는 디스크의 다음 위치에 있습니다.

```
/opt/plugins/var/log/pan/plugin_cisco_trustsec.log /opt/plugins/
var/log/pan/plugin_cisco_trustsec_sub.log /opt/plugins/var/
log/pan/plugin_cisco_trustsec_ret.log /opt/plugins/var/log/pan/
plugin_cisco_trustsec_proc.log
```

 ©2024 Palo Alto Networks, Inc.

Panorama 디바이스에 설치된 모든 플러그인에서 공유하는 로그 파일의 크기 제한은 1,000만 바이트입니다. 로그 파일은 93,000개의 세션 로그인을 허용할 수 있습니다. 로그 순환을 구성하는 경우 백업 로그는 186,000개의 세션 로그인을 지원할 수 있습니다.

- 플러그인 디버그 수준을 변경합니다.

```
request plugins debug level $level plugin-name cisco_trustsec
```

  - 꺼짐: 디버그 로그가 없습니다.
  - 낮음: 기본 디버그 로그만 덤프합니다.
  - 중간: 세부 디버그 로그를 덤프합니다.
  - 높음: 요청/응답 메시지를 포함한 모든 것을 서버에 덤프합니다.
- 로그를 단일 로그 파일로 병합:

```
request plugins cisco_trustsec merge-logs
```

- CLI에 디버그 로그 표시:
  - Panorama 10.0.0 이전 버전에 설치된 Cisco TrustSec 플러그인 버전 1.0.2 이상:

```
tail mp-log plugin_cisco_trustsec_merged.log
```

  - Panorama 버전 10.0.0 이상에 설치된 Cisco TrustSec 플러그인 버전 1.0.2 이상:

```
tail follow yes plugins-log
```


©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

문제 해결

다음 주제는 Panorama™ 관리 서버 및 전용 로그 수집기에 대한 문제를 해결합니다.

- Panorama 시스템 문제 해결
- 로그 저장소 및 연결 문제 해결
- RMA 방화벽 교체
- 커밋 실패 문제 해결
- 등록 또는 일련번호 오류 문제 해결
- 보고 오류 문제 해결
- 디바이스 관리 라이선스 오류 문제 해결
- 자동으로 되돌린 방화벽 구성 문제 해결
- 작업 성공 또는 실패 상태 보기
- 관리되는 디바이스에 대한 정책 일치 및 연결 테스트
- 관리되는 방화벽에 대한 통계 덤프 파일 생성
- Panorama에 대한 관리 디바이스 연결 복구
- 만료된 디바이스 인증서 복원

Panorama 시스템 문제 해결

- Panorama에 대한 진단 파일 생성
- Panorama 정지 상태 진단
- 파일 시스템 무결성 검사 모니터링
- 소프트웨어 및 콘텐츠 업데이트를 위한 Panorama Storage 관리
- Panorama HA 배포의 스플릿 브레인에서 복구
- 메모리 문제로 인한 Panorama 재부팅

Panorama에 대한 진단 파일 생성

진단 파일은 시스템 활동을 모니터링하고 Panorama 문제의 잠재적 원인을 식별하는 데 도움이 됩니다. Palo Alto Networks 기술 지원에서 문제 해결을 지원하기 위해 지원 담당자가 기술 지원 파일을 요청할 수 있습니다. 다음 절차에서는 기술 지원 파일을 다운로드하여 지원 사례에 업로드하는 방법을 설명합니다.

STEP 1 | **Panorama** > 지원을 선택한 다음 기술 지원 파일 생성을 클릭합니다.

STEP 2 | 파일을 다운로드하여 컴퓨터에 저장합니다.

STEP 3 | Palo Alto Networks 고객 지원 웹 사이트에서 귀하의 케이스에 파일을 업로드하십시오.

Panorama 정지 상태 진단

Panorama가 일시 중단된 상태인 경우 다음 조건을 확인하십시오.

- 일련번호 - 각 Panorama 가상 어플라이언스의 일련번호가 고유한지 확인합니다. 동일한 일련번호를 사용하여 두 개 이상의 Panorama 인스턴스를 생성하는 경우 동일한 일련번호를 사용하는 모든 인스턴스가 일시 중단됩니다.
- 모드 - Panorama 가상 어플라이언스를 고가용성(HA) 구성으로 배포하는 경우 두 HA 피어가 동일한 모드에 있는지 확인합니다. Panorama 모드 또는 레거시 모드.
- **HA** 우선 순위 - 한 피어에서 HA 우선 순위 설정을 기본으로, 다른 피어에서 보조로 설정했는지 확인합니다. 우선 순위 설정이 두 피어 모두에서 동일하면 일련번호에서 더 높은 숫자 값을 가진 Panorama 피어가 일시 중단된 상태가 됩니다.
- **Panorama** 소프트웨어 버전 - 두 Panorama HA 피어가 동일한 Panorama 소프트웨어 버전(주 및 부 버전 번호)을 실행하고 있는지 확인합니다.

파일 시스템 무결성 검사 모니터링

Panorama는 정기적으로 FSCK(파일 시스템 무결성 검사)를 수행하여 Panorama 시스템 파일의 손상을 방지합니다. 이 검사는 8번의 재부팅 후 또는 마지막 FSCK가 실행된 후 90일 후에 발생하는 재부팅 시 수행됩니다. Panorama가 FSCK를 실행 중인 경우 웹 인터페이스 및 SSH(Secure Shell) 로그인 화면에 FSCK가 진행 중임을 나타내는 경고가 표시됩니다. 이 프로세스가 완료될 때까지 로그인할 수 없습니다. 이 프로세스를 완료하는 데 걸리는 시간은 스토리지 시스템의 크기에 따라 다릅니다. 크기에 따라 Panorama에 다시 로그인하려면 몇 시간이 걸릴 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

Panorama 또는 관리 방화벽에 PAN-OS 소프트웨어 업데이트를 성공적으로 다운로드하여 설치한 후 PAN-OS 소프트웨어 무결성을 보장하기 위해 소프트웨어 설치 프로세스의 일부로 Panorama 또는 관리 방화벽이 재부팅된 후 소프트웨어 업데이트가 검증됩니다. 이렇게 하면 현재 실행 중인 소프트웨어 업데이트가 양호한 것으로 알려져 있고 원격 또는 물리적 악용으로 인해 Panorama 또는 관리 방화벽이 손상되지 않습니다.

FSCK에서 진행 상황을 보려면 Panorama에 대한 콘솔 액세스를 설정하고 상태를 봅니다.

소프트웨어 및 콘텐츠 업데이트를 위한 Panorama Storage 관리

Panorama™ 관리 서버를 사용하여 Panorama용 콘텐츠 및 소프트웨어 업데이트 설치, 방화벽 업그레이드, 로그 수집기 업그레이드를 수행할 수 있습니다. 업데이트를 저장하기 위해 Panorama에서 사용 가능한 공간을 구성할 수 없습니다. 할당된 저장 용량이 90%에 도달하면 Panorama는 새 다운로드 또는 업로드를 위한 공간을 확보(저장된 업데이트 삭제)하도록 경고합니다. 최대 업데이트 수는 Panorama가 저장하는 모든 업데이트에 적용되는 전역 설정입니다. 이 설정을 구성하려면 CLI에 액세스해야 합니다. 기본값은 각 유형의 두 업데이트입니다.

- 각 유형의 최대 업데이트 수를 수정합니다.

  Panorama CLI에 액세스하고 다음을 입력합니다. 여기서 *<number>*은(는) 2에서 64 사이일 수 있습니다.

  ```
  > set max-num-images count <number>
  ```

- Panorama가 현재 저장하는 업데이트 수를 봅니다.

  다음을 입력합니다:

  ```
  > show max-num-images
  ```

- 웹 인터페이스를 사용하여 업데이트를 삭제하여 Panorama의 공간을 확보하십시오.
  1. 삭제할 업데이트 유형 선택:
     - 방화벽 또는 로그 수집기 업데이트:

       PAN-OS/Panorama 소프트웨어 이미지 - **Panorama** > **Device Deployment** > **Software**를 선택합니다.

       GlobalProtect™ 에이전트/앱 소프트웨어 업데이트 - **Panorama** > **Device Deployment** > **GlobalProtect Client**를 선택합니다.

       콘텐츠 업데이트 - **Panorama** > **Device** 배포 > 동적 업데이트를 선택합니다.
     - Panorama 소프트웨어 이미지 - **Panorama** > 소프트웨어를 선택합니다.
     - Panorama 콘텐츠 업데이트 - **Panorama** > 동적 업데이트를 선택합니다.
  2. 이미지 또는 업데이트의 맨 오른쪽 열에 있는 **X** 아이콘을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

- CLI를 사용하여 업데이트를 삭제하여 Panorama의 공간을 확보하십시오.

  버전별 소프트웨어 이미지 삭제:

  ```
  > delete software version <version_number>
  ```

  콘텐츠 업데이트 삭제:

  ```
  > delete content update <filename>
  ```

Panorama HA 배포의 스플릿 브레인에서 복구

Panorama가 고가용성(HA) 설정으로 구성된 경우 관리되는 방화벽은 활성 및 수동 Panorama HA 피어 모두에 연결됩니다. 활성 및 수동 Panorama 피어 간의 연결이 실패하면 수동 Panorama가 활성 피어 역할을 인계받기 전에 활성 피어와 수동 피어 모두에 방화벽이 연결되어 있는지 확인합니다. 하나의 방화벽이라도 두 피어에 연결되어 있으면 페일오버가 트리거되지 않습니다.

방화벽 집합이 활성 피어에 연결되고 방화벽 집합이 수동 피어에 연결될 때 페일오버가 트리거되는 드문 경우이지만 두 피어에 연결된 방화벽이 없는 경우를 스플릿 브레인이라고 합니다. 스플릿 브레인이 발생하면 다음 조건이 발생합니다.

- Panorama 피어는 다른 피어의 상태나 HA 역할을 알지 못합니다.
- 두 Panorama 피어가 모두 활성화되고 고유한 방화벽 집합을 관리합니다.

스플릿 브레인을 해결하려면 네트워크 문제를 디버그하고 Panorama HA 피어 간의 연결을 복원하십시오.

그러나 피어 간의 연결을 복원하지 않고 방화벽의 구성을 변경해야 하는 경우 다음과 같은 몇 가지 옵션이 있습니다.

- 두 Panorama 피어에 동일한 구성 변경 사항을 수동으로 추가합니다. 이렇게 하면 링크가 다시 설정될 때 구성이 동기화됩니다.
- 하나의 Panorama 위치에서만 구성을 추가/변경해야 하는 경우 재구성된 Panorama 피어 간의 링크가 다시 연결될 때 변경하고 구성을 동기화합니다(변경한 피어에서 동기화를 시작해야 함). 피어를 동기화하려면 대시보드 탭을 선택한 다음 고가용성 위젯에서 피어에 동기화 링크를 클릭하십시오.
- 각 위치에서 연결된 방화벽에 대해서만 구성을 추가/변경해야 하는 경우 각 Panorama 피어에서 개별적으로 구성을 변경할 수 있습니다. 피어의 연결이 끊어졌기 때문에 복제가 없으며 이제 각 피어에는 완전히 다른 구성 파일이 있습니다(동기화되지 않음). 따라서 연결이 복원될 때 각 피어의 구성 변경 사항이 손실되지 않도록 하기 위해 구성이 자동으로 다시 동기화되도록 허용할 수 없습니다. 이 문제를 해결하려면 각 Panorama 피어에서 구성을 내보내고 외부 비교 및 병합 도구를 사용하여 변경 사항을 수동으로 병합하십시오. 변경 사항이 통합되면 기본 Panorama에서 통합 구성 파일을 불러온 다음 불러온 구성 파일을 피어와 동기화할 수 있습니다.

메모리 문제로 인한 Panorama 재부팅

수시로 Panorama™ 관리 서버의 구성 관리 및 작동을 담당하는 내부 `configd` 프로세스에서 메모리 문제가 발생할 수 있습니다. 이러한 메모리 문제로 인해 Panorama 성능 저하, 시스템 충돌 또는 Panorama 기능에 영향을 줄 수 있는 기타 작동 오류가 발생할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

PAN-OS 11.1 및 이후 릴리즈에서는 `configd` 프로세스에서 Panorama를 재부팅하도록 지시하는 등의 메모리 문제가 발생하면 중요한 시스템 로그(모니터 > 로그 > 시스템)가 생성됩니다. `configd` 프로세스에서 메모리 문제가 발생할 때 Panorama를 자동으로 재부팅하는 대신 가장 빠른 시간에 Panorama를 재부팅할 수 있으므로 진행 중인 작업을 완료하고 의도하지 않았거나 예상치 못한 Panorama 재부팅으로 인한 운영 부담을 줄일 수 있습니다.

Panorama가 `configd` 메모리 문제로 인해 Panoroama를 다시 시작하기 위해 중요한 시스템 로그를 정기적으로 생성하는 경우 Palo Alto Networks는 Palo Alto Networks 지원에 문의하여 문제를 해결하고 진단하기 위해 Panorama에 대한 진단 파일을 생성할 것을 권장합니다.

 ©2024 Palo Alto Networks, Inc.

로그 저장소 및 연결 문제 해결

로그 마이그레이션은 *M*-시리즈 어플라이언스에서만 지원됩니다. *Panorama* 가상 어플라이언스를 마이그레이션하려면 Panorama 가상 어플라이언스를 다른 하이퍼바이저로 마이그레이션을(를) 참조하십시오.

- Panorama 포트 사용 확인
- 수집기 그룹에 대한 Zero Log Storage 해결
- M-시리즈 어플라이언스에서 장애가 발생한 디스크 교체
- ESXi 서버에서 가상 디스크 교체
- vCloud Air에서 가상 디스크 교체
- 로그 수집기 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션
- Panorama 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션
- 고가용성의 Panorama 모드에서 새로운 M-시리즈 어플라이언스 모델로 로그 마이그레이션
- 고가용성의 Panorama 모드에서 동일한 M 시리즈 어플라이언스 모델로 로그 마이그레이션
- 비HA Panorama의 실패/RMA 후 로그 수집기 마이그레이션
- M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성
- 로그 쿼리 작업 보기

Panorama 포트 사용 확인

Panorama가 관리 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터, 고가용성(HA) 피어와 통신할 수 있도록 하려면 다음 표를 사용하여 네트워크에서 열어야 하는 포트를 확인하십시오. Panorama는 포트 통신에 TCP 프로토콜을 사용합니다.

기본적으로 Panorama는 관리(MGT) 인터페이스를 사용하여 디바이스(방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터)를 관리하고, 로그를 수집하고, 수집기 그룹과 통신하고, 디바이스에 소프트웨어 및 콘텐츠 업데이트를 배포합니다. 그러나 Panorama 6.1~7.1을 실행하는 M-700, M-600, M-500, M-300 또는 M-200 어플라이언스의 Eth1 또는 Eth2 인터페이스에 로그 수집 및 수집기 그룹 통신 기능을 선택적으로 할당할 수 있습니다. 어플라이언스가 Panorama 8.0 이상의 버전을 실행하는 경우 M-700, M-600, M-500, M-300 또는 M-200 어플라이언스의 Eth1, Eth2, Eth3, Eth4 또는 Eth5 인터페이스에 기능을 할당할 수 있습니다. 다음 표에 나열된 포트는 인터페이스에 할당하는 기능에 관계없이 적용됩니다. 예를 들어 로그 수집을 MGT에 할당하고 수집기 그룹 통신을 Eth2에 할당하면 MGT는 포트 3978을 사용하고 Eth2는 포트 28270을 사용합니다. (Panorama 가상 어플라이언스는 이러한 모든 기능에 대해 MGT 인터페이스만 사용할 수 있습니다.)

 ©2024 Palo Alto Networks, Inc.

커뮤니케이션 체계 및 연계 구축 방향	**Panorama 5.x**에서 사용되는 포트	**Panorama 6.x ~ 7.x**에서 사용되는 포트	**Panorama 8.x** 이상에서 사용되는 포트	설명
Panorama 및 Panorama(HA) 방향: 각 피어는 다른 피어에 대한 자체 연결을 시작합니다.	28	28	28	암호화가 활성화된 경우 HA 연결 및 동기화용입니다. 로그 배포를 위해 수집기 그룹의 로그 수집기 간의 통신에 사용됩니다.
Panorama 및 Panorama(HA) 방향: 각 피어는 다른 피어에 대한 자체 연결을 시작합니다.	28769 및 28260(5.1) 28769 및 49160(5.0)	28260 및 28769	28260 및 28769	암호화가 활성화되지 않은 경우 HA 연결 및 동기화용입니다.
Panorama 및 관리 방화벽 방향: 방화벽에 의해 시작됨	3978	3978	3978	로그가 방화벽에서 Panorama로 포워딩되는 양방향 연결. 구성 변경 사항은 Panorama에서 관리되는 방화벽으로 푸시됩니다. 컨텍스트 전환 명령은 동일한 연결을 통해 전송됩니다.
Panorama 및 로그 수집기 방향: 로그 수집기에 의해 시작됨	3978	3978	3978	관리 및 로그 수집/보고용. Panorama 모드의 Panorama에 있는 로컬 로그 수집기 간의 통신 및 분산 로그 수집 배포의 로그 수집기와 통신하는 데 사용됩니다.
Panorama 및 관리 디바이스(방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터) 방향: • PAN-OS 8.x 이상의 버전을 실행하는 관리 디바이스에 의해 시작됩니다. • PAN-OS 7.x 또는 이전 버전을 실행하는 디바이	3978	3978	28443	PAN-OS 8.x 이상의 버전을 실행하는 디바이스는 포트 28443을 사용하여 Panorama에서 소프트웨어 및 콘텐츠 업데이트 파일을 검색합니다. 7.x 또는 이전 버전을 실행하는 디바이스는 Panorama에서 업데이트 파일을 검색하지 않습니다. Panorama는 포트 3978을 통해 업데이트 파일을 디바이스로 푸시합니다.

©2024 Palo Alto Networks, Inc.

커뮤니케이션 체계 및 연계 구축 방향	Panorama 5.x에서 사용되는 포트	Panorama 6.x ~ 7.x에서 사용되는 포트	Panorama 8.x 이상에서 사용되는 포트	설명
스에 대해 Panorama에서 시작되었습니다.				WildFire 어플라이언스 및 어플라이언스 클러스터의 Panorama 관리를 지원하려면 관리되는 WildFire 어플라이언스에 PAN-OS 8.0.1 이상이 설치되어 있어야 합니다. Panorama는 8.0.1 이상의 버전을 실행하여 WildFire 어플라이언스 및 어플라이언스 클러스터를 관리하는 것이 좋습니다.
로그 수집기 - 로그 수집기 방향: 각 로그 수집기는 수집기 그룹의 다른 로그 수집기에 대한 연결을 시작합니다.	49190	28270	28270	로그 수집기 간에 블록 및 모든 바이너리 데이터를 배포하는 데 사용됩니다.
Panorama - Strata Logging Service	NA	NA	444 버전 *8.0.5* 이상.	Strata Logging Service와 통신 보안 채널을 설정합니다. 관리형 방화벽은 포트 3978을 사용하여 Strata Logging Service와 통신합니다.

수집기 그룹에 대한 Zero Log Storage 해결

디스크 쌍이 로그 수집기에서 로깅을 위해 활성화되지 않은 경우 수집기 그룹의 로그 스토리지 용량이 0MB로 표시될 수 있습니다. 디스크 쌍을 활성화하려면 수집기 그룹의 각 로그 수집기에 대해 다음 단계를 수행합니다.

STEP 1 | RAID 디스크 쌍을 추가합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 수집기 이름을 클릭합니다.
2. 디스크를 선택한 다음 각 RAID 디스크 쌍을 추가하고 확인을 클릭합니다.

STEP 2 | Panorama에 변경 사항을 커밋하고 Collector Group에 변경 사항을 푸시합니다.

1. 커밋 > 커밋 후 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 수집기 그룹을 선택한 다음 수정한 수집기 그룹을 선택한 다음 확인을 클릭합니다.
3. 변경 사항을 커밋하고 푸시합니다.

©2024 Palo Alto Networks, Inc.

STEP 3 | 로그 수집기 및 디스크 쌍의 상태를 확인합니다.

1. **Panorama** > 관리형 수집기를 선택한 다음 각 로그 수집기의 구성이 Panorama와 동기화되었는지 확인합니다.

   구성 상태 열은 동기화 중으로 표시되어야 하고 런타임 상태 열은 연결됨으로 표시되어야 합니다.
2. 각 로그 수집기의 마지막 열에서 통계를 클릭하고 디스크 쌍이 활성화 및 사용 가능 상태인지 확인합니다.

M-시리즈 어플라이언스에서 장애가 발생한 디스크 교체

M-시리즈 어플라이언스에서 디스크에 오류가 발생하면 디스크를 교체하고 RAID 1 어레이에서 재구성해야 합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.

ESXi 서버에서 가상 디스크 교체

VMware ESXi 서버에서 실행되는 Panorama 가상 어플라이언스에 가상 디스크를 추가한 후에는 가상 디스크의 크기를 조정할 수 없습니다. Legacy 모드의 Panorama 가상 어플라이언스는 하나의 로그 저장 위치만 허용하므로 다음과 같이 가상 디스크를 교체하여 로그 저장 용량을 수정해야 합니다. Panorama 모드에서는 Panorama 가상 어플라이언스에서 로그 스토리지 용량 확장에 다른 디스크(최대 12개)를 추가하기만 하면 됩니다.

레거시 모드의 *Panorama* 가상 어플라이언스에서 교체하면 기존 디스크의 로그가 손실됩니다. 기존 로그를 보존하는 옵션은 레거시 모드에서 Panorama 가상 어플라이언스에 스토리지를 추가할 때 기존 로그 보존을(를) 참조하십시오.

STEP 1 | 이전 가상 디스크를 제거합니다.

1. VMware vSphere Client에 액세스하고 가상 머신 탭을 선택합니다.
2. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 끄기를 선택합니다.
3. Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 설정 편집을 선택합니다.
4. 하드웨어 탭에서 가상 디스크를 선택한 다음 제거를 클릭합니다.
5. 제거 옵션 중 하나를 선택하고 확인을 클릭합니다.

STEP 2 | 새 가상 디스크를 추가합니다.

1. ESXi 서버의 Panorama에 가상 디스크 추가.

   ESXi 5.5 이상의 버전에서 실행되는 Panorama는 최대 8TB의 가상 디스크를 지원합니다. 이전 ESXi 버전에서 실행되는 Panorama는 최대 2TB의 가상 디스크를 지원합니다.
2. vSphere Client에서 Panorama 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭하고 전원 > 전원 켜기를 선택합니다.

   재부팅 프로세스에는 몇 분이 소요될 수 있으며 ### # ## ## ###가 표시됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | 수정된 로그 저장 용량이 올바른지 확인합니다.

1. Panorama 가상 어플라이언스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 리포팅 세팅 섹션의 로그 스토리지 필드에 수정된 로그 저장 용량이 정확하게 표시되는지 확인합니다.

vCloud Air에서 가상 디스크 교체

VMware vCloud Air에서 실행되는 Panorama 가상 어플라이언스에 가상 디스크를 추가한 후에는 가상 디스크의 크기를 조정할 수 없습니다. Legacy 모드의 Panorama 가상 어플라이언스는 하나의 로그 저장 위치만 허용하므로 다음과 같이 가상 디스크를 교체하여 로그 저장 용량을 수정해야 합니다. Panorama 모드에서는 간단하게(최대 12개까지) vCloud Air의 Panorama에 가상 디스크 추가을(를) 할 수 있습니다.

레거시 모드의 *Panorama* 가상 어플라이언스에서 교체하면 기존 디스크의 로그가 손실됩니다. 기존 로그를 보존하는 옵션은 레거시 모드에서 Panorama 가상 어플라이언스에 스토리지를 추가할 때 기존 로그 보존을(를) 참조하십시오.

STEP 1 | 이전 가상 디스크를 제거합니다.

1. vCloud Air 웹 콘솔에 액세스하고 **Virtual Private Cloud OnDemand** 지역을 선택합니다.
2. 가상 머신 탭에서 Panorama 가상 어플라이언스를 선택합니다.
3. 작업 > 리소스 편집을 선택합니다.
4. 제거할 가상 디스크에 대해 **x**를 클릭합니다.

STEP 2 | 새 가상 디스크를 추가합니다.

1. 다른 디스크를 추가합니다.
2. 스토리지를 최대 8TB로 설정하고 스토리지 계층을 표준 또는 **SSD** 가속으로 설정합니다.
3. 변경 내용을 저장합니다.

STEP 3 | 재부팅 Panorama.

1. Panorama 가상 어플라이언스에 로그인합니다.
2. **Panorama** > 설정 > 작업 및 **Panorama** 재부팅을 선택합니다.

STEP 4 | 수정된 로그 저장 용량이 올바른지 확인합니다.

1. 재부팅 후 Panorama 가상 어플라이언스에 로그인합니다.
2. **Panorama** > 설정 > 관리를 선택한 다음 로깅 및 리포팅 세팅 섹션의 로그 스토리지 필드에 수정된 로그 저장 용량이 정확하게 표시되는지 확인합니다.

로그 수집기 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션

로그 수집기 모드(전용 로그 수집기)에서 M-Series 어플라이언스를 교체해야 하는 경우 RAID 디스크를 새 M-Series 어플라이언스로 이동하여 방화벽에서 수집한 로그를 마이그레이션할 수 있습니다. 이 절차는 다음에 대해 지원됩니다.

- M-Series 어플라이언스에서 시스템 오류가 발생한 후 로그 복구 및 동일한 M-Series 어플라이언스 모델로 마이그레이션

 ©2024 Palo Alto Networks, Inc.

- M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션
- M-200 어플라이언스에서 M-600 어플라이언스로 마이그레이션

M-Series 어플라이언스에서 로깅 디스크를 제거하고 *M-600 Panorama* 관리 서버에 로드하여 로그를 마이그레이션하는 것은 지원되지 않습니다. *M-600* 어플라이언스로 마이그레이션하려면 M-600 어플라이언스를 설정하고 새 M-600 어플라이언스에 대한 로그 포워딩을 구성하고 *M*-시리즈 어플라이언에 저장된 로그에 더 이상 액세스할 필요가 없을 때까지 M-시리즈 어플라이언스를 관리되는 로그 수집기로 구성합니다.

STEP 1 | 전용 로그 수집기가 될 새 M-시리즈 어플라이언스의 초기 설정을 수행합니다.

1. M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성 수행.

   인터페이스를 구성할 때 관리*(MGT)* 인터페이스만 구성하십시오. 로그 수집기 모드*(*이 절차 뒷부분*)*로 전환하면 다른 인터페이스에 대한 구성이 제거됩니다. *Log Collector*가 *MGT* 이외의 인터페이스를 사용하는 경우 *Log Collector*를 구성할 때 추가합니다*(*2단계 참조*).*
3. Panorama를 등록합니다.
4. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 동일한 하드웨어 모델인 경우에만 다음과 같이 Panorama 지원 라이선스를 구매 및 활성화하거나 라이선스를 양도하십시오. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 다른 모델인 경우 새 라이선스를 구입해야 합니다.
   1. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
   2. 자산 탭을 선택한 다음 스페어 링크를 클릭합니다.
   3. 새 M-시리즈 어플라이언스의 일련번호를 클릭합니다.
   4. 라이선스 전송을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

5. 이전 M-시리즈 어플라이언스를 선택하고 제출을 클릭합니다.

5. 방화벽 관리 라이선스를 활성화합니다. M-200 어플라이언스에서 M-600 어플라이언스로 마이그레이션하는 경우 마이그레이션 라이선스와 연결된 인증 코드를 입력합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
7. Panorama 모드에서 로그 수집기 모드로 전환:
   1. Log Collector CLI에 액세스하고 Log Collector 모드로 전환합니다.

      ```
      > request system system-mode logger
      ```

   2. **Y**를 입력하여 모드 변경을 확인합니다. M-시리즈 어플라이언스가 재부팅됩니다. 재부팅 프로세스가 터미널 에뮬레이션 소프트웨어 세션을 종료하는 경우 M-시리즈 어플라이언스에 다시 연결하여 Panorama 로그인 프롬프트를 표시하십시오.

      CMS ***###*** 프롬프트가 표시되면 사용자 이름이나 암호를 입력하지 않고 *Enter* 키를 누릅니다.
8. 로그 수집기 CLI를 사용하여 로그 수집기와 Panorama 관리 서버 간의 연결을 활성화합니다. <IPaddress1 is for the MGT interface of the primary Panorama and <IPaddress2>은(는) 보조 Panorama의 MGT 인터페이스용입니다.

   ```
   > configure # set deviceconfig system panorama-
   server <IPaddress1> panorama-server-2 <IPaddress2> # commit
    # exit
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama 관리 서버에서 새 로그 수집기를 관리 수집기로 추가합니다.

일련번호가 필요한 명령이 있는 모든 단계의 경우 전체 일련번호를 입력해야 합니다. *Tab* 키를 눌러도 부분 일련번호가 완성되지 않습니다.

1. Panorama 웹 인터페이스를 사용하거나 다음 CLI 명령을 사용하여 로그 수집기를 관리형 수집기로 구성합니다.

```
> configure # set log-collector <LC_serial_number>
  deviceconfig system hostname <LC_hostname> # exit
```

이전 로그 수집기가 로그 수집 및 수집기 그룹 통신을 위해 *MGT* 인터페이스 이외의 인터페이스를 사용한 경우 관리 수집기로 구성할 때 새 로그 수집기에서 해당 인터페이스를 정의해야 합니다(***Panorama*** > 관리형 수집기 > ***Interfaces***).

2. 변경 사항을 Panorama에 커밋합니다. 아직 수집기 그룹에 변경 사항을 커밋하지 마십시오.

```
> configure # commit # exit
```

3. Log Collector가 Panorama에 연결되어 있고 해당 디스크 쌍의 상태가 존재/사용 가능한지 확인합니다.

```
> show log-collector serial-number <log-collector_SN>
```

디스크 쌍은 복원 프로세스의 이 단계에서 비활성화된 것으로 표시됩니다.

STEP 3 | 이전 로그 수집기에서 RAID 디스크를 제거합니다.

1. 시스템이 종료될 때까지 전원 버튼을 눌러 이전 로그 수집기의 전원을 끕니다.
2. 디스크 쌍을 제거합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 마이그레이션을 위해 디스크를 준비합니다.

각 디스크 쌍에 대한 메타데이터를 생성하면 인덱스가 다시 작성됩니다. 따라서 데이터 크기에 따라 이 프로세스를 완료하는 데 시간이 오래 걸릴 수 있습니다. 프로세스를 가속화하기 위해 여러 *CLI* 세션을 시작하고 각 세션에서 메타데이터 재생성 명령을 실행하여 모든 쌍에 대해 동시에 프로세스를 완료할 수 있습니다. 자세한 내용은 M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성을 참조하십시오.

1. 새 로그 수집기에 디스크를 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

   M-200 어플라이언스의 디스크 캐리어는 *M-600* 어플라이언스의 디스크 캐리어와 호환되지 않습니다. 따라서 이러한 하드웨어 모델 간에 마이그레이션할 때 새 어플라이언스에 디스크를 삽입하기 전에 이전 캐리어에서 각 디스크의 나사를 풀고 새 캐리어에 디스크를 삽입해야 합니다.

   디스크 쌍 연결을 유지해야 합니다. 이전 어플라이언스의 슬롯 A1/A2에서 새 어플라이언스의 슬롯 B1/B2로 디스크 쌍을 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.
2. 각 쌍에 대해 다음 CLI 명령을 실행하여 디스크 쌍을 활성화하십시오.

   ```
   > request system raid add <slot> force no-format
   ```

   예:

   ```
   > request system raid add A1 force no-format > request system
     raid add A2 force no-format
   ```

   force 및 **no-format** 인수가 필요합니다. **force** 인수는 디스크 쌍을 새 로그 수집기와 연결합니다. **no-format** 인수는 드라이브의 재포맷을 방지하고 디스크에 저장된 로그를 유지합니다.
3. 각 디스크 쌍에 대한 메타데이터를 생성합니다.

   ```
   > request metadata-regenerate slot <slot_number>
   ```

   예:

   ```
   > request metadata-regenerate slot 1
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | Collector Group에 디스크가 없는 Log Collector를 추가합니다.

이 시점부터 *Panorama* 및 *Log Collectors*에서 마이그레이션 프로세스를 완료하는 데 필요한 커밋만 수행합니다. 다른 변경 작업을 보류하십시오.

1. Panorama CLI에 액세스.
2. 디스크가 없는 로그 수집기를 수집기 그룹에 추가할 수 있도록 Panorama 제한 덮어쓰기:
   request log-migration-set-start

STEP 6 | 로그를 마이그레이션합니다.

이 단계에서는 웹 인터페이스가 아니라 *Panorama CLI*를 사용해야 합니다.

이전 로그 수집기를 포함하는 수집기 그룹에 새 로그 수집기를 할당해야 합니다.

1. Collector Group에 새 Log Collector를 할당하고 Panorama에 변경 사항을 커밋합니다.

```
> configure # set log-collector-group <collector_group_name>
 logfwd-setting collectors <new_LC_serial_number> # commit
 # exit
```

2. 각 디스크 쌍에 대해 이전 로그 수집기에서 새 로그 수집기로 로그를 마이그레이션하고 디스크 쌍을 새 로그 수집기에 연결합니다.

```
> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

예:

```
> request log-migration from 003001000010 old-disk-pair A to
 00300100038 new-disk-pair A
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 수집기 그룹을 재구성합니다.

1. 웹 인터페이스를 사용하여 로그를 포워딩하는 방화벽에 새 로그 수집기를 할당합니다(**Panorama** > 수집기 그룹 > 디바이스 로그 포워딩). 방화벽 기본 설정 목록에서 새 로그 수집기에 이전 로그 수집기와 동일한 우선 순위를 부여합니다.

   *CLI*를 사용하여 방화벽 기본 설정 목록의 우선 순위 할당을 변경할 수 없습니다.

2. 수집기 그룹에서 이전 로그 수집기를 삭제합니다.

   ```
   > configure # delete log-collector-group <group_name> logfwd-
   setting collectors <old_LC_serial_number>
   ```

   예:

   ```
   # delete log-collector-group DC-Collector-Group logfwd-setting
    collectors 003001000010
   ```

3. Panorama 구성에서 이전 Log Collector를 삭제하고 Panorama에 변경 사항을 커밋합니다.

   ```
   # delete log-collector <old_LC_serial_number> # commit # exit
   ```

4. 관리되는 방화벽이 새 로그 수집기로 로그를 보낼 수 있도록 수집기 그룹 변경 사항을 커밋합니다.

   ```
   > commit-all log-collector-config log-collector-
   group <collector_group_name>
   ```

   예:

   ```
   > commit-all log-collector-config log-collector-group DC-
   Collector-Group
   ```

STEP 8 | 새 전용 로그 수집기에서 새 키를 생성합니다.

이 명령은 새 로그 수집기를 수집기 그룹에 추가하는 데 필요하며 교체할 로그 수집기의 수집기 그룹에 대해서만 실행해야 합니다. 이 단계에서는 기존 *RSA* 키를 삭제하고 *Panorama*에서 새 *RSA* 키를 생성할 수 있습니다.

1. Panorama CLI에 액세스합니다.
2. 새 로그 수집기에서 모든 RSA 키 삭제:

   request logdb update-collector-group-after-replace collector-group <collector-group-name>

   프로세스를 완료하는 데 최대 10분이 소요될 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 수집기 그룹의 모든 로그 수집기에 대해 SearchEngine 상태가 활성인지 확인합니다.

수집기 그룹의 모든 로그 수집기에 대해 *SearchEngine* 상태가 활성이 될 때까지 계속하지 마십시오. 그러면 교체되는 로그 수집기에서 로그가 제거됩니다.

1. Panorama CLI에 액세스.
2. 다음 명령을 실행하여 로그 수집기 세부 정보를 표시합니다.
   - 모든 로그 수집기에 대한 Panorama:

     ## ### ## ##

     또는 각 전용 로그 수집기에서 다음 명령을 실행할 수 있습니다.

     ```
     show log-collector detail
     ```
3. SearchEngine 상태가 활성인지 확인합니다.

```
Redistribution status: none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status: ####
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14
 09:58:19
```

STEP 10 | 새 로그 수집기에서 이전 로그 수집기 일련번호를 새 로그 수집기 일련번호로 바꿉니다.

이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체해야 새 Log Collector가 문제를 제거하기 위해 실행되지 않아 Log Collector가 필요할 때 마이그레이션된 로그에서 이전 데이터를 제거할 수 없습니다.

1. 로그 수집기 CLI에 액세스합니다.
2. 이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체합니다.

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

Panorama 모드에서 새 M-시리즈 어플라이언스로 로그 마이그레이션

Panorama 모드(Panorama 관리 서버)에서 M-Series 어플라이언스를 교체해야 하는 경우 RAID 디스크를 새 M-Series 어플라이언스로 이동하여 방화벽에서 수집한 로그를 마이그레이션할 수 있습니다. 이 절차는 다음에 대해 지원됩니다.

- M-Series 어플라이언스에서 시스템 오류가 발생한 후 로그 복구 및 동일한 M-Series 어플라이언스 모델로 마이그레이션
- M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션

 ©2024 Palo Alto Networks, Inc.

- M-200 어플라이언스에서 M-600 어플라이언스로 마이그레이션

> M-Series 어플라이언스에서 로깅 디스크를 제거하고 *M-600 Panorama* 관리 서버에 로드하여 로그를 마이그레이션하는 것은 지원되지 않습니다. *M-600* 어플라이언스로 마이그레이션하려면 M-600 어플라이언스를 설정하고 새 M-600 어플라이언스로의 로그 포워딩을 구성하고 *M*-시리즈 어플라이언스에 저장된 로그에 더 이상 액세스할 필요가 없을 때까지 M-시리즈 어플라이언스를 관리되는 로그 수집기로 구성합니다.

이 마이그레이션 절차에서는 HA 구성이 아닌 단일 M 시리즈 어플라이언스를 수집기 그룹의 관리 수집기(로그 수집기)로 교체하는 다음 시나리오를 다룹니다.

STEP 1 | 보존하려는 경우 이전 M-시리즈 어플라이언스의 SSD에 있는 모든 로그를 외부 대상으로 포워딩합니다.

SSD는 Panorama 및 Log Collector가 생성하는 시스템 및 구성 로그를 저장합니다. M-시리즈 어플라이언스 간에 SSD를 이동할 수 없습니다.

Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.

STEP 2 | Panorama 모드에서 폐기된 M-시리즈 어플라이언스에서 Panorama 구성을 내보냅니다.

1. Panorama 어플라이언스에 로그인하고 **Panorama** > 설정 > 작업를 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.

STEP 3 | 이전 M-시리즈 어플라이언스에서 RAID 디스크를 제거합니다.

1. 시스템이 종료될 때까지 전원 버튼을 눌러 기존 M-시리즈 어플라이언스의 전원을 끕니다.
2. 디스크 쌍을 제거합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

STEP 4 | 새 M-시리즈 어플라이언스의 초기 설정을 수행합니다.

1. M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성 수행.
3. Panorama를 등록합니다.
4. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 동일한 하드웨어 모델인 경우에만 다음과 같이 Panorama 지원 라이선스를 구매 및 활성화하거나 라이선스를 이전하십시오. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 다른 모델인 경우 새 라이선스를 구입해야 합니다.

    1. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
    2. 자산 탭을 선택한 다음 스페어 링크를 클릭합니다.
    3. 새 M-시리즈 어플라이언스의 일련번호를 클릭합니다.
    4. 라이선스 전송을 클릭합니다.
    5. 이전 M-시리즈 어플라이언스를 선택하고 제출을 클릭합니다.

 ©2024 Palo Alto Networks, Inc.

5. 방화벽 관리 라이선스를 활성화합니다. M-200 어플라이언스에서 M-600 어플라이언스로 마이그레이션하는 경우 마이그레이션 라이선스와 연결된 인증 코드를 입력합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.

STEP 5 | 폐기된 M-시리즈 어플라이언스에서 내보낸 Panorama 구성 스냅샷을 Panorama 모드의 새 M-시리즈 어플라이언스로 로드합니다.

1. 새 M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인을(를) 선택하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 사용 중지된 M 시리즈 어플라이언스에서 내보낸 구성 파일을 찾은 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키(Panorama의 마스터 키)를 선택한 다음 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

   *RMA Panorama*를 교체하려면 명명된 *Panorama* 구성 스냅숏을 로드할 때 규칙 ***UUID***를 유지해야 합니다. 이 옵션을 선택하지 않으면 *Panorama*는 구성 스냅숏에서 이전 규칙 *UUID*를 모두 제거하고 *Panorama*의 규칙에 새 *UUID*를 할당하므로 정책 규칙 적중 수와 같은 이전 *UUID*와 관련된 정보를 유지하지 않습니다.
4. 필요에 따라 추가 구성 변경을 수행합니다.

   이전 *M-Series* 어플라이언스가 *Panorama* 서비스에 대해 *MGT* 인터페이스 이외의 인터페이스(예: 로그 수집)를 사용한 경우 새 *M-Series* 어플라이언스(***Panorama*** > ***Setup*** > ***Interfaces***)에서 해당 인터페이스를 정의해야 합니다.
5. 커밋 > **Panorama**에 커밋을 선택한 다음 커밋을 확인합니다. 계속하기 전에 오류를 해결합니다.
6. Panorama 구성에 대한 변경 사항을 커밋합니다.

STEP 6 | 새 M 시리즈 어플라이언스에 디스크를 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

M-200 어플라이언스의 디스크 캐리어는 *M-600* 어플라이언스의 디스크 캐리어와 호환되지 않습니다. 따라서 이러한 하드웨어 모델 간에 마이그레이션할 때 새 어플라이언스에 디스크를 삽입하기 전에 이전 캐리어에서 각 디스크의 나사를 풀고 새 캐리어에 디스크를 삽입해야 합니다.

디스크 쌍 연결을 유지해야 합니다. 이전 어플라이언스의 슬롯 A1/A2에서 새 어플라이언스의 슬롯 B1/B2로 디스크 쌍을 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.

STEP 7 | 폐기된 M 시리즈 어플라이언스에서 새 M 시리즈 어플라이언스로 로그 수집기 그룹 메타데이터를 복사하고 mgmtsrvr 프로세스를 다시 시작하려면 Palo Alto Networks 고객 지원에 문의하십시오.

Palo Alto Networks TAC 엔지니어와 작업할 때 Palo Alto Networks 기술 자료를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | M-시리즈 어플라이언스가 수집기 그룹의 일부인 경우 사용 중지된 M-시리즈 어플라이언스 일련번호가 여전히 올바른 수집기 그룹의 일부인지 확인합니다.

```
debug log-collector-group show name <Log Collector Group name>
```

폐기된 M-시리즈 어플라이언스 일련번호가 더 이상 올바른 수집기 그룹의 일부가 아닌 경우 이전 단계에서 기술 지원 폴더가 잘못 복사된 것입니다. 기술 지원 폴더를 올바른 위치에 복사하려면 Palo Alto Networks 고객 지원에 다시 문의하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 마이그레이션을 위해 디스크를 준비합니다.

각 디스크 쌍에 대한 메타데이터를 생성하면 인덱스가 다시 작성됩니다. 따라서 데이터 크기에 따라 이 프로세스를 완료하는 데 시간이 오래 걸릴 수 있습니다. 프로세스를 가속화하기 위해 여러 *CLI* 세션을 시작하고 각 세션에서 메타데이터 재생성 명령을 실행하여 모든 쌍에 대해 동시에 프로세스를 완료할 수 있습니다. 자세한 내용은 M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성을 참조하십시오.

1. 새 M 시리즈 어플라이언스에 디스크를 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

   M-200 어플라이언스의 디스크 캐리어는 *M-600* 어플라이언스의 디스크 캐리어와 호환되지 않습니다. 따라서 이러한 하드웨어 모델 간에 마이그레이션할 때 새 어플라이언스에 디스크를 삽입하기 전에 이전 캐리어에서 각 디스크의 나사를 풀고 새 캐리어에 디스크를 삽입해야 합니다.

   디스크 쌍 연결을 유지해야 합니다. 이전 어플라이언스의 슬롯 A1/A2에서 새 어플라이언스의 슬롯 B1/B2로 디스크 쌍을 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.
2. 각 쌍에 대해 다음 CLI 명령을 실행하여 디스크 쌍을 활성화하십시오.

   ```
   admin> request system raid add <slot> force no-format
   ```

   예:

   ```
   admin> request system raid add A1 force no-format
    admin> request system raid add A2 force no-format
   ```

   force 및 **no-format** 인수가 필요합니다. **force** 인수는 디스크 쌍을 새 어플라이언스와 연결합니다. **no-format** 인수는 드라이브의 재포맷을 방지하고 디스크에 저장된 로그를 유지합니다.
3. 각 디스크 쌍에 대한 메타데이터를 생성합니다.

   이 단계는 디스크의 로그 데이터 양에 따라 최대 *6*시간이 소요될 수 있습니다.

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   예:

   ```
   admin> request metadata-regenerate slot 1
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 새 M-시리즈 어플라이언스에서 로컬 로그 수집기를 구성합니다.

> 일련번호가 필요한 명령이 있는 모든 단계의 경우 전체 일련번호를 입력해야 합니다. *Tab* 키를 눌러도 부분 일련번호가 완성되지 않습니다.

이 시점에서 새 M-시리즈 어플라이언스에서 디스크를 활성화하지 마십시오. 로그를 성공적으로 마이그레이션하면 Panorama가 자동으로 디스크를 활성화합니다.

1. Panorama 웹 인터페이스를 사용하거나 다음 CLI 명령을 사용하여 로컬 로그 수집기를 관리형 수집기로 구성합니다.

```
admin> configure admin# set log-collector <log-collector_SN>
 deviceconfig system hostname <log-collector-hostname>
 admin# exit
```

2. 로컬 로그 수집기가 Panorama에 연결되어 있고 해당 디스크 쌍의 상태가 존재/사용 가능한지 확인합니다.

```
admin> show log-collector serial-number <log-collector_SN>
```

   디스크 쌍은 복원 프로세스의 이 단계에서 비활성화된 것으로 표시됩니다.

3. 변경 사항을 Panorama에 커밋합니다. 아직 수집기 그룹에 변경 사항을 커밋하지 마십시오.

```
admin> configure admin# commit
```

STEP 11 | Collector Group에 디스크가 없는 Log Collector를 추가합니다.

> 이 시점부터 *Panorama* 및 *Log Collectors*에서 마이그레이션 프로세스를 완료하는 데 필요한 커밋만 수행합니다. 다른 변경 작업을 보류하십시오.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 디스크가 없는 로그 수집기를 수집기 그룹에 추가할 수 있도록 Panorama 제한 덮어쓰기: **request log-migration-set-start**
3. 덮어쓴 제한을 커밋합니다.

```
admin> configure admin# commit force
```

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 로그를 마이그레이션합니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. Collector Group의 구성원으로 새 로컬 Log Collector를 추가하고 Panorama에 변경 사항을 커밋합니다.

```
admin# set log-collector-group <collector_group_name> logfwd-
setting collectors <SN_managed_collector> admin# commit
 admin# exit
```

구성에서 삭제하지 않았기 때문에 이전 로컬 로그 수집기가 구성원 목록에 계속 나타납니다.

3. 각 디스크 쌍에 대해 로그를 새 어플라이언스로 마이그레이션합니다.

```
admin> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

예:

```
admin> request log-migration from 003001000010 old-disk-pair A
 to 00300100038 new-disk-pair A
```

4. Panorama에 변경 사항을 커밋합니다.

```
admin> configure admin# commit
```

 ©2024 Palo Alto Networks, Inc.

STEP 13 | 수집기 그룹을 재구성합니다.

1. 로그를 포워딩하는 방화벽(**Panorama** > 수집기 그룹 > 디바이스 로그 포워딩)에 새 로그 수집기를 할당하기 위한 새 M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인. 방화벽 기본 설정 목록에서 새 로그 수집기에 이전 로그 수집기와 동일한 우선 순위를 부여합니다.

   *CLI*를 사용하여 방화벽 기본 설정 목록의 우선 순위 할당을 변경할 수 없습니다.

2. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
3. 수집기 그룹에서 이전 로그 수집기를 삭제합니다.

   ```
   admin# delete log-collector-group <group_name> logfwd-setting
    collectors <old_LC_serial_number>
   ```

   예:

   ```
   admin# delete log-collector-group DC-Collector-Group logfwd-
   setting collectors 003001000010
   ```

4. Panorama 구성에서 이전 Log Collector를 삭제하고 Panorama에 변경 사항을 커밋합니다.

   ```
   admin# delete log-collector <old_LC_serial_number>
    admin# commit admin# exit
   ```

5. 관리되는 방화벽이 새 로그 수집기로 로그를 보낼 수 있도록 수집기 그룹 변경 사항을 커밋합니다.

   ```
   admin> commit-all log-collector-config log-collector-
   group <collector_group_name>
   ```

   예:

   ```
   admin> commit-all log-collector-config log-collector-group DC-
   Collector-Group
   ```

STEP 14 | 새 로그 수집기에서 새 키를 생성합니다.

이 명령은 새 로그 수집기를 수집기 그룹에 추가하는 데 필요하며 교체할 로그 수집기의 수집기 그룹에 대해서만 실행해야 합니다. 이 단계에서는 기존 *RSA* 키를 삭제하고 *Panorama*에서 새 *RSA* 키를 생성할 수 있습니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 새 로그 수집기에서 모든 RSA 키를 삭제합니다.

   request logdb update-collector-group-after-replace collector-group <collector-group-name>

   프로세스를 완료하는 데 최대 10분이 소요될 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 15 | 수집기 그룹의 모든 로그 수집기에 대해 SearchEngine 상태가 활성인지 확인합니다.

수집기 그룹의 모든 로그 수집기에 대해 *SearchEngine* 상태가 활성이 될 때까지 계속하지 마십시오. 그러면 교체되는 로그 수집기에서 로그가 제거됩니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 다음 명령을 실행하여 로그 수집기 세부 정보를 표시합니다.
   - 모든 로그 수집기에 대한 Panorama:

     ```
     ## ### ## ##
     ```

     또는 각 전용 로그 수집기에서 다음 명령을 실행할 수 있습니다.

     ```
     show log-collector detail
     ```
3. SearchEngine 상태가 활성인지 확인합니다.

```
Redistribution status: none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status: ####
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14
 09:58:19
```

STEP 16 | 새 로그 수집기에서 이전 로그 수집기 일련번호를 새 로그 수집기 일련번호로 바꿉니다.

이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체해야 새 Log Collector가 문제를 제거하기 위해 실행되지 않아 Log Collector가 필요할 때 마이그레이션된 로그에서 이전 데이터를 제거할 수 없습니다.

1. 로그 수집기 CLI에 액세스합니다.
2. 이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체합니다.

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

고가용성의 Panorama 모드에서 새로운 M-시리즈 어플라이언스 모델로 로그 마이그레이션

Panorama 모드(Panorama 관리 서버)에서 M-700, M-600, M-500, M-300, M-200 또는 M-100 어플라이언스를 교체할 M 시리즈 어플라이언스와 다른 M 시리즈 어플라이언스로 교체해야 하는 경우 다음을 마이그레이션할 수 있습니다. RAID 디스크를 새 M 시리즈 어플라이언스로 이동하여 방화벽에서 수집한 로그를 기록합니다. 디스크를 이동하면 하드웨어 업그레이드(M-100 어플라이언스에서 M-500 어플라이언스로)의 일부로 로그를 마이그레이션할 수 있습니다. M-100 어플라이언스를 M-500 어플라이언스 간

 ©2024 Palo Alto Networks, Inc.

에 마이그레이션할 수 있습니다. M-100 및 M-500 어플라이언스는 M-200 또는 M-600 어플라이언스 간에 마이그레이션할 수 없습니다.

> M-Series 어플라이언스에서 로깅 디스크를 제거하고 *M-600 Panorama* 관리 서버에 로드하여 로그를 마이그레이션하는 것은 지원되지 않습니다. *M-600* 어플라이언스로 마이그레이션하려면 M-600 어플라이언스를 설정하고 새 M-600 어플라이언스에 대한 로그 포워딩을 구성하고 *M*-시리즈 어플라이언에 저장된 로그에 더 이상 액세스할 필요가 없을 때까지 M-시리즈 어플라이언스를 관리되는 로그 수집기로 구성합니다.

이 마이그레이션 절차에서는 다음 시나리오를 다룹니다.

- 하나의 Panorama HA 피어에는 수집기 그룹에 관리 수집기(로그 수집기)가 있습니다.

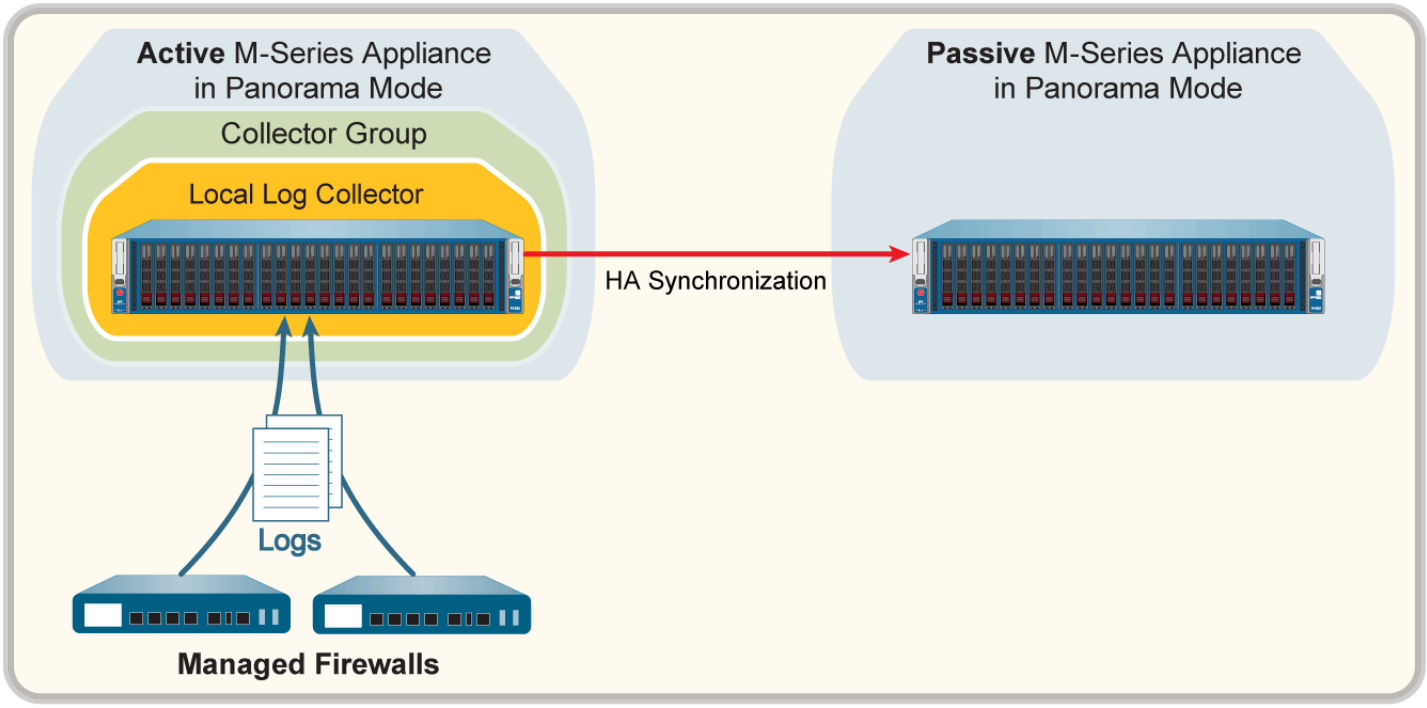


그림 **29: Collector** 그룹이 있는 **Panorama HA** 피어

- 두 Panorama HA 피어에는 단일 수집기 그룹에 속하는 관리 수집기가 있습니다. 자세한 내용은 수집기 그룹당 여러 로컬 로그 수집기를 참조하세요.
- 두 Panorama HA 피어에는 관리되는 수집기가 있으며 각각은 별도의 수집기 그룹에 할당됩니다. 자세한 내용은 수집기 그룹당 단일 로컬 로그 수집기를 참조하세요.

STEP 1 | 보존하려는 경우 이전 M-시리즈 어플라이언스의 SSD에 있는 모든 로그를 외부 대상으로 포워딩합니다.

SSD는 Panorama 및 Log Collector가 생성하는 시스템 및 구성 로그를 저장합니다. M-시리즈 어플라이언스 간에 SSD를 이동할 수 없습니다.

Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama 모드의 사용 중지된 기본 M-시리즈 어플라이언스에서 Panorama 구성을 내보냅니다.

1. 교체할 M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인을(를) 선택한 다음 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 저장을 클릭하고 구성을 식별할 이름을 입력한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 내보내기를 클릭하고 방금 저장한 구성의 이름을 선택한 다음 확인을 클릭합니다. Panorama는 구성을 XML 파일로 클라이언트 시스템에 내보냅니다.

STEP 3 | 이전 M-시리즈 어플라이언스에서 RAID 디스크를 제거합니다.

1. 시스템이 종료될 때까지 전원 버튼을 눌러 기존 M-시리즈 어플라이언스의 전원을 끕니다.
2. 디스크 쌍을 제거합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

STEP 4 | 새 M-시리즈 어플라이언스의 초기 설정을 수행합니다.

HA 구성의 새 M-시리즈 어플라이언스 각각에 대해 이 단계를 반복합니다.

1. M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성 수행.
3. Panorama를 등록합니다.
4. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 동일한 하드웨어 모델인 경우에만 다음과 같이 Panorama 지원 라이선스를 구매 및 활성화하거나 라이선스를 이전하십시오. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 다른 모델인 경우 새 라이선스를 구입해야 합니다.
   1. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
   2. 자산 탭을 선택한 다음 스페어 링크를 클릭합니다.
   3. 새 M-시리즈 어플라이언스의 일련번호를 클릭합니다.
   4. 라이선스 전송을 클릭합니다.
   5. 이전 M-시리즈 어플라이언스를 선택하고 제출을 클릭합니다.
5. 방화벽 관리 라이선스를 활성화합니다. M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션하는 경우 마이그레이션 라이선스와 연결된 인증 코드를 입력합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
7. Panorama에서 HA 설정. 새 M 시리즈 어플라이언스는 교체하려는 HA 피어와 우선 순위가 동일해야 합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 기본 해제된 M-시리즈 어플라이언스에서 내보낸 Panorama 구성 스냅샷을 Panorama 모드의 새 기본 M-시리즈 어플라이언스로 로드합니다.

1. 새 M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인을(를) 선택하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 사용 중지된 M 시리즈 어플라이언스에서 내보낸 구성 파일을 찾은 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 구성의 이름을 선택한 다음 복호화 키(Panorama의 마스터 키)를 선택한 다음 확인을 클릭합니다. Panorama는 로드된 구성으로 현재 후보 구성을 덮어씁니다. Panorama는 구성 파일을 로드할 때 발생하는 모든 오류를 표시합니다. 오류가 발생하면 로컬 파일에 저장하십시오. 마이그레이션된 구성이 유효한지 확인하려면 각 오류를 해결하십시오.

   *RMA Panorama*를 교체하려면 명명된 *Panorama* 구성 스냅숏을 로드할 때 규칙 ***UUID***를 유지해야 합니다. 이 옵션을 선택하지 않으면 *Panorama*는 구성 스냅숏에서 이전 규칙 *UUID*를 모두 제거하고 *Panorama*의 규칙에 새 *UUID*를 할당하므로 정책 규칙 적중 수와 같은 이전 *UUID*와 관련된 정보를 유지하지 않습니다.
4. 필요에 따라 추가 구성 변경을 수행합니다.

   이전 *M-Series* 어플라이언스가 *Panorama* 서비스에 대해 *MGT* 인터페이스 이외의 인터페이스*(*예*:* 로그 수집*)*를 사용한 경우 새 *M-Series* 어플라이언스*(****Panorama*** > ***Setup*** > ***Interfaces****)*에서 해당 인터페이스를 정의해야 합니다.
5. 커밋 > **Panorama**에 커밋을 선택한 다음 커밋을 확인합니다. 계속하기 전에 오류를 해결합니다.
6. Panorama 구성에 대한 변경 사항을 커밋합니다. 커밋되면 Panorama 구성이 HA 피어 간에 동기화됩니다.

STEP 6 | 새 M 시리즈 어플라이언스에 디스크를 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

HA 구성의 새 M-시리즈 어플라이언스 각각에 대해 이 단계를 반복합니다.

M-100 어플라이언스의 디스크 캐리어는 *M-500* 어플라이언스의 디스크 캐리어와 호환되지 않습니다. 따라서 이러한 하드웨어 모델 간에 마이그레이션할 때 새 어플라이언스에 디스크를 삽입하기 전에 이전 캐리어에서 각 디스크의 나사를 풀고 새 캐리어에 디스크를 삽입해야 합니다.

디스크 쌍 연결을 유지해야 합니다. 이전 어플라이언스의 슬롯 A1/A2에서 새 어플라이언스의 슬롯 B1/B2로 디스크 쌍을 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.

STEP 7 | 폐기된 M 시리즈 어플라이언스에서 새 M 시리즈 어플라이언스로 로그 수집기 그룹 메타데이터를 복사하고 mgmtsrvr 프로세스를 다시 시작하려면 Palo Alto Networks 고객 지원에 문의하십시오.

Palo Alto Networks TAC 엔지니어와 작업할 때 Palo Alto Networks 기술 자료를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 8 | M-시리즈 어플라이언스가 수집기 그룹의 일부인 경우 사용 중지된 M-시리즈 어플라이언스 일련번호가 여전히 올바른 수집기 그룹의 일부인지 확인합니다.

```
debug log-collector-group show name <Log CollectorGroup name>
```

폐기된 M-시리즈 어플라이언스 일련번호가 더 이상 올바른 수집기 그룹의 일부가 아닌 경우 이전 단계에서 기술 지원 폴더가 잘못 복사된 것입니다. 기술 지원 폴더를 올바른 위치에 복사하려면 Palo Alto Networks 고객 지원에 다시 문의하십시오.

STEP 9 | 마이그레이션을 위해 디스크를 준비합니다.



각 디스크 쌍에 대한 메타데이터를 생성하면 인덱스가 다시 작성됩니다. 따라서 데이터 크기에 따라 이 프로세스를 완료하는 데 시간이 오래 걸릴 수 있습니다. 프로세스를 가속화하기 위해 여러 *CLI* 세션을 시작하고 각 세션에서 메타데이터 재생성 명령을 실행하여 모든 쌍에 대해 동시에 프로세스를 완료할 수 있습니다. 자세한 내용은 M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성을 참조하십시오.

1. 각 쌍에 대해 다음 CLI 명령을 실행하여 디스크 쌍을 활성화하십시오.

   ```
   admin> request system raid add <slot> force no-format
   ```

   예:

   ```
   admin> request system raid add A1 force no-format
    admin> request system raid add A2 force no-format
   ```

   force 및 **no-format** 인수가 필요합니다. **force** 인수는 디스크 쌍을 새 어플라이언스와 연결합니다. **no-format** 인수는 드라이브의 재포맷을 방지하고 디스크에 저장된 로그를 유지합니다.
2. 각 디스크 쌍에 대한 메타데이터를 생성합니다.

   디스크의 로그 데이터 양에 따라 이 단계를 완료하는 데 최대 *60*시간이 소요될 수 있습니다. 새 *M-Series* 어플라이언스는 *###* 상태여야 합니다. *Panorama*가 *## ###* 상태인 경우 할당된 로그 수집기 *ID*를 가져오는 데 문제가 발생할 수 있습니다.

   새 *M-Series* 어플라이언스가 *### HA* 피어인 경우 현재 *### HA* 피어의 Panorama 웹 인터페이스에 로그인하고 ***Panorama*** **>** 고가용성 및 고가용성을 위해 로컬 ***Panorama*** 일시 중단을 선택합니다.

   로그를 성공적으로 마이그레이션한 후 고가용성을 위해 로컬 ***Panorama*** 기능을 설정합니다.

   ```
   admin> request metadata-regenerate slot <slot_number>
   ```

   예:

   ```
   admin> request metadata-regenerate slot 1
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 새 M-시리즈 어플라이언스에서 로컬 로그 수집기를 구성합니다.

> 일련번호가 필요한 명령이 있는 모든 단계의 경우 전체 일련번호를 입력해야 합니다. *Tab* 키를 눌러도 부분 일련번호가 완성되지 않습니다.

이 시점에서 새 M-시리즈 어플라이언스에서 디스크를 활성화하지 마십시오. 로그를 성공적으로 마이그레이션하면 Panorama가 자동으로 디스크를 활성화합니다.

1. Panorama 웹 인터페이스를 사용하거나 다음 CLI 명령을 사용하여 로컬 로그 수집기를 관리형 수집기로 구성합니다.

```
admin> configure admin# set log-collector <log-collector_SN>
 deviceconfig system hostname <log-collector-hostname>
 admin# exit
```

2. 변경 사항을 Panorama에 커밋합니다. 아직 수집기 그룹에 변경 사항을 커밋하지 마십시오.

```
admin> configure admin# commit
```

3. 로컬 로그 수집기가 Panorama에 연결되어 있고 해당 디스크 쌍의 상태가 존재/사용 가능한지 확인합니다.

```
admin> show log-collector serial-number <log-collector_SN>
```

디스크 쌍은 복원 프로세스의 이 단계에서 비활성화된 것으로 표시됩니다.

STEP 11 | Collector Group에 디스크가 없는 Log Collector를 추가합니다.

> 이 시점부터 *Panorama* 및 *Log Collectors*에서 마이그레이션 프로세스를 완료하는 데 필요한 커밋만 수행합니다. 다른 변경 작업을 보류하십시오.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 디스크가 없는 로그 수집기를 수집기 그룹에 추가할 수 있도록 Panorama 제한 덮어쓰기: **request log-migration-set-start**
3. Panorama에 변경 사항을 커밋합니다.

```
admin> configure admin# commit force
```

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 로그를 마이그레이션합니다.

새 *M* 시리즈 어플라이언스는 로그 마이그레이션을 #### ## ## *HA* 피어여야 합니다. 새 *M* 시리즈 어플라이언스의 경우 ## *HA* 피어의 Panorama 웹 인터페이스에 로그인하고 ***Panorama*** **>** 고가용성 및 고가용성을 위해 로컬 ***Panorama*** 일시 중단을 선택합니다.

로그를 성공적으로 마이그레이션한 후 고가용성을 위해 로컬 ***Panorama*** 기능을 설정합니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. Collector Group의 구성원으로 새 로컬 Log Collector를 추가하고 Panorama에 변경 사항을 커밋합니다.

```
admin# set log-collector-group <collector_group_name> logfwd-
setting collectors <SN_managed_collector> admin# commit
 admin# exit
```

구성에서 삭제하지 않았기 때문에 이전 로컬 로그 수집기가 구성원 목록에 계속 나타납니다.

3. 각 디스크 쌍에 대해 로그를 새 어플라이언스로 마이그레이션합니다.

```
admin> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

예:

```
admin> request log-migration from 003001000010 old-disk-pair A
 to 00300100038 new-disk-pair A
```

4. Panorama에 변경 사항을 커밋합니다.

```
admin> configure admin# commit
```

 ©2024 Palo Alto Networks, Inc.

STEP 13 | 수집기 그룹을 재구성합니다.

1. 로그를 포워딩하는 방화벽(**Panorama** > 수집기 그룹 > 디바이스 로그 포워딩)에 새 로그 수집기를 할당하기 위한 새 M 시리즈 어플라이언스의 Panorama 웹 인터페이스에 로그인. 방화벽 기본 설정 목록에서 새 로그 수집기에 이전 로그 수집기와 동일한 우선 순위를 부여합니다.

   *CLI*를 사용하여 방화벽 기본 설정 목록의 우선 순위 할당을 변경할 수 없습니다.

2. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
3. 수집기 그룹에서 이전 로그 수집기를 삭제합니다.

   ```
   admin# delete log-collector-group <group_name> logfwd-setting
    collectors <old_LC_serial_number>
   ```

   예:

   ```
   admin# delete log-collector-group DC-Collector-Group logfwd-
   setting collectors 003001000010
   ```

4. Panorama 구성에서 이전 Log Collector를 삭제하고 Panorama에 변경 사항을 커밋합니다.

   ```
   admin# delete log-collector <old_LC_serial_number>
    admin# commit admin# exit
   ```

5. 관리되는 방화벽이 새 로그 수집기로 로그를 보낼 수 있도록 수집기 그룹 변경 사항을 커밋합니다.

   ```
   admin> commit-all log-collector-config log-collector-
   group <collector_group_name>
   ```

   예:

   ```
   admin> commit-all log-collector-config log-collector-group DC-
   Collector-Group
   ```

STEP 14 | 새 로그 수집기에서 새 키를 생성합니다.

이 명령은 새 로그 수집기를 수집기 그룹에 추가하는 데 필요하며 교체할 로그 수집기의 수집기 그룹에 대해서만 실행해야 합니다. 이 단계에서는 기존 *RSA* 키를 삭제하고 *Panorama*에서 새 *RSA* 키를 생성할 수 있습니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 새 로그 수집기에서 모든 RSA 키를 삭제합니다.

   request logdb update-collector-group-after-replacecollector-group <collector-group-name>

   프로세스를 완료하는 데 최대 10분이 소요될 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

STEP 15 | 수집기 그룹의 모든 로그 수집기에 대해 SearchEngine 상태가 활성인지 확인합니다.

수집기 그룹의 모든 로그 수집기에 대해 *SearchEngine* 상태가 활성이 될 때까지 계속하지 마십시오. 그러면 교체되는 로그 수집기에서 로그가 제거됩니다.

1. 새 M 시리즈 어플라이언스의 Panorama CLI에 액세스합니다.
2. 다음 명령을 실행하여 로그 수집기 세부 정보를 표시합니다.
   - 모든 로그 수집기에 대한 Panorama:

     ```
     ## ### ## ##
     ```

     또는 각 전용 로그 수집기에서 다음 명령을 실행할 수 있습니다.

     ```
     show log-collector detail
     ```
3. SearchEngine 상태가 활성인지 확인합니다.

```
Redistribution status: none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status: ####
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14
 09:58:19
```

STEP 16 | 새 로그 수집기에서 이전 로그 수집기 일련번호를 새 로그 수집기 일련번호로 바꿉니다.

이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체해야 새 Log Collector가 문제를 제거하기 위해 실행되지 않아 Log Collector가 필요할 때 마이그레이션된 로그에서 이전 데이터를 제거할 수 없습니다.

1. 로그 수집기 CLI에 액세스합니다.
2. 이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체합니다.

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

 ©2024 Palo Alto Networks, Inc.

STEP 17 | 새 보조 Panorama 고가용성 피어를 설정합니다.

1. 보존하려는 경우 이전 M 시리즈 어플라이언스의 SSD에 있는 모든 로그를 외부 대상으로 포워딩합니다.
2. 이전 M 시리즈 어플라이언스에서 RAID 디스크를 제거합니다.
3. 새 M 시리즈 어플라이언스의 초기 설정을 수행합니다.
4. 새 M 시리즈 어플라이언스에 디스크를 삽입합니다.
5. 7~16단계를 반복하여 이전 M 시리즈 어플라이언스에서 새 M 시리즈 어플라이언스로 로그를 마이그레이션합니다.
6. Panorama에서 HA 설정. 새 M 시리즈 어플라이언스는 교체하려는 HA 피어와 우선 순위가 동일해야 합니다.
7. 기본 HA 피어의 Panorama 웹 인터페이스에 로그인을(를) 수행하고 대시보드 > 고가용성 > 동기화를 클릭하여 M 시리즈 어플라이언스 HA 피어의 구성을 동기화합니다.

고가용성의 Panorama 모드에서 동일한 M 시리즈 어플라이언스 모델로 로그 마이그레이션

Panorama 모드(Panorama 관리 서버)의 고가용성(HA) 구성으로 배포된 M-700, M-600, M-500, M-300, M-200 또는 M-100 어플라이언스를 M 시리즈 어플라이언스와 동일한 M 시리즈 어플라이언스로 교체해야 하는 경우 시리즈 어플라이언스가 교체되면 RAID 디스크를 새 M 시리즈 어플라이언스로 이동하여 방화벽에서 수집한 로그를 마이그레이션할 수 있습니다. 디스크를 이동하면 M-시리즈 어플라이언스에서 시스템 오류가 발생한 후 로그를 복구할 수 있습니다.

이 마이그레이션 절차에서는 다음 시나리오를 다룹니다.

- 하나의 Panorama HA 피어에는 수집기 그룹에 관리 수집기(로그 수집기)가 있습니다.

 ©2024 Palo Alto Networks, Inc.

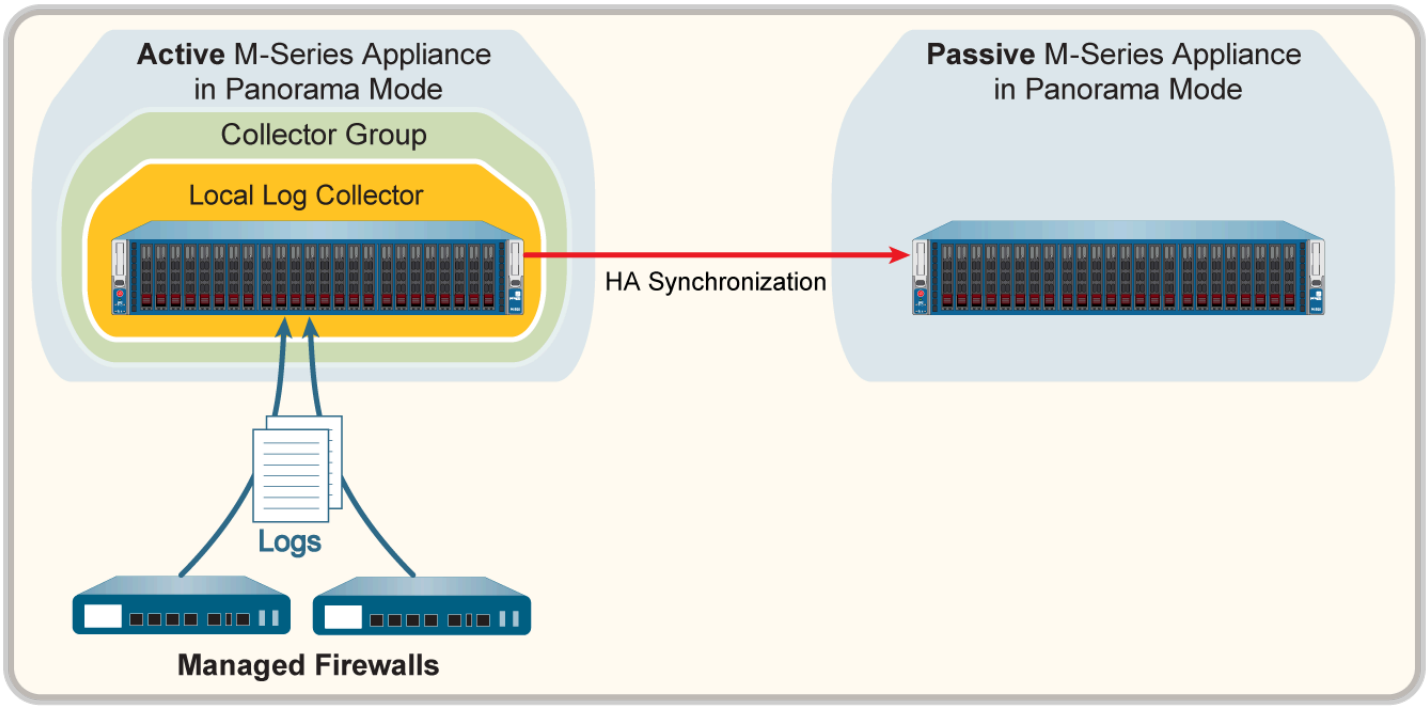


그림 **30: Collector** 그룹이 있는 **Panorama HA** 피어

- 두 Panorama HA 피어에는 단일 수집기 그룹에 속하는 관리 수집기가 있습니다. 자세한 내용은 수집기 그룹당 여러 로컬 로그 수집기를 참조하세요.
- 두 Panorama HA 피어에는 관리되는 수집기가 있으며 각각은 별도의 수집기 그룹에 할당됩니다. 자세한 내용은 수집기 그룹당 단일 로컬 로그 수집기를 참조하세요.

STEP 1 | 보존하려는 경우 이전 M-시리즈 어플라이언스의 SSD에 있는 모든 로그를 외부 대상으로 포워딩합니다.

SSD는 Panorama 및 Log Collector가 생성하는 시스템 및 구성 로그를 저장합니다. M-시리즈 어플라이언스 간에 SSD를 이동할 수 없습니다.

Panorama에서 외부 대상으로의 로그 포워딩을 구성합니다.

STEP 2 | (활성 기본 HA 피어의 RMA만 해당) Panorama HA 피어의 고가용성 구성을 재구성하여 RMA 프로세스 중에 ## HA 피어를 ## HA 피어로 만듭니다.

이 단계는 A/P HA 구성에서 ## HA 피어를 교체하여 보안 통신 상태를 재설정하고 새 M 시리즈 어플라이언스의 CA(인증 기관)가 HA 구성의 기존 피어와 실수로 동기화되지 않도록 하는 데 필요합니다. #

 ©2024 Palo Alto Networks, Inc.

HA 피어를 교체할 때 HA 선택 설정을 재구성하면 RMA 프로세스 중에 디바이스의 Panorama 관리가 중단되지 않은 상태로 유지됩니다.

A/P HA 구성에서## HA 피어를 교체하는 경우 이 단계를 건너뜁니다.

1. ## HA 피어의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 고가용성을 선택하고 일렉션(Election) 설정을 수정합니다.
3. 우선 순위에 대해 보조를 선택하고 확인을 클릭합니다.
4. 커밋 및 **Panorama**에 커밋을 선택합니다.
   교체 중인 Panorama HA 피어는 이제 ## HA 피어입니다.
5. ## HA 피어의 Panorama 웹 인터페이스에 로그인.
6. **Panorama** > 고가용성을 선택하고 일렉션(Election) 설정을 수정합니다.
7. 우선 순위에 대해 기본을 선택하 고확인을 클릭합니다.
8. 커밋 및 **Panorama**에 커밋을 선택합니다.
   이전 ## Panorama는 이제 ## HA 피어입니다.

STEP 3 | 교체하려는 Panorama HA 피어에서 HA 기능을 일시 중단합니다.

보안 통신 상태 재설정 및 새 M 시리즈 어플라이언스의 CA(인증 기관)가 RMA 프로세스 중에 HA 구성의 기존 피어와 실수로 동기화되지 않도록 하려면 단계가 필요합니다. 그러면 Panorama HA 피어가 # # ## 상태가 됩니다.

1. 교체하려는 Panorama HA 피어의 Panorama 웹 인터페이스에 로그인.
2. 고가용성을 위해 **Panorama** > 고가용성 및 로컬 **Panorama** 일시 중단을 선택합니다.
3. 확인을 클릭하여 Panorama HA 피어에서 HA 일시 중단을 확인합니다.

STEP 4 | 교체하려는 Panorama HA 피어에서 보안 연결 설정을 재설정합니다.

1. 교체하려는 Panorama HA 피어의 Panorama CLI에 로그인.
2. 보안 연결 상태를 재설정합니다.

   이 명령은 모든 관리형 디바이스의 연결을 재설정하며 되돌릴 수 없습니다.

   ```
   admin> request sc3 reset
   ```

3. 교체하려는 Panorama HA 피어에서 관리 서버를 다시 시작합니다.

   ```
   admin> debug software restart process management-server
   ```

STEP 5 | 이전 M-시리즈 어플라이언스에서 RAID 디스크를 제거합니다.

1. 시스템이 종료될 때까지 전원 버튼을 눌러 기존 M-시리즈 어플라이언스의 전원을 끕니다.
2. 디스크 쌍을 제거합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 6 | 새 M-시리즈 어플라이언스의 초기 설정을 수행합니다.

1. M 시리즈 어플라이언스를 랙에 장착합니다. 지침은 M 시리즈 어플라이언스 하드웨어 참조 가이드를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성 수행.

   이전 *M* 시리즈 어플라이언스가 *Panorama* 서비스에 대해 *MGT* 인터페이스 이외의 인터페이스*(*예*:* 로그 수집*)*를 사용한 경우 새 *M* 시리즈 어플라이언스*(**Panorama** >* 설정 > 인터페이스*)*의 초기 구성 중에 해당 인터페이스를 정의해야 합니다.
3. Panorama를 등록합니다.
4. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 동일한 하드웨어 모델인 경우에만 다음과 같이 Panorama 지원 라이선스를 구매 및 활성화하거나 라이선스를 이전하십시오. 새 M 시리즈 어플라이언스가 이전 M 시리즈 어플라이언스와 다른 모델인 경우 새 라이선스를 구입해야 합니다.

   1. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
   2. 자산 탭을 선택한 다음 스페어 링크를 클릭합니다.
   3. 새 M-시리즈 어플라이언스의 일련번호를 클릭합니다.
   4. 라이선스 전송을 클릭합니다.
   5. 이전 M-시리즈 어플라이언스를 선택하고 제출을 클릭합니다.
5. 방화벽 관리 라이선스를 활성화합니다. M-100 어플라이언스에서 M-500 어플라이언스로 마이그레이션하는 경우 마이그레이션 라이선스와 연결된 인증 코드를 입력합니다.
6. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.
7. 필요에 따라 추가 구성 변경을 수행합니다.

   이전 *M-Series* 어플라이언스가 *Panorama* 서비스에 대해 *MGT* 인터페이스 이외의 인터페이스*(*예*:* 로그 수집*)*를 사용한 경우 새 *M-Series* 어플라이언스*(**Panorama** > **Setup** > **Interfaces**)*에서 해당 인터페이스를 정의해야 합니다.
8. Panorama에서 HA 설정. 새 M 시리즈 어플라이언스는 교체하려는 HA 피어와 우선 순위가 동일해야 합니다.

   새 *M* 시리즈 어플라이언스는 *##* HA 피어로 *HA* 구성에 추가해야 합니다. 새 *M* 시리즈를 *##* HA 피어로 추가하면 재설정 보안 통신 설정 상태가 기존 *M* 시리즈 어플라이언스에 강제로 동기화되어 디바이스의 *Panorama* 관리가 중단됩니다.

 ©2024 Palo Alto Networks, Inc.

STEP 7 | 새 M 시리즈 어플라이언스에 디스크를 삽입합니다. 자세한 내용은 M-시리즈 어플라이언스 하드웨어 참조 가이드의 디스크 교체 절차를 참조하십시오.

> *M-100* 어플라이언스의 디스크 캐리어는 *M-500* 어플라이언스의 디스크 캐리어와 호환되지 않습니다. 따라서 이러한 하드웨어 모델 간에 마이그레이션할 때 새 어플라이언스에 디스크를 삽입하기 전에 이전 캐리어에서 각 디스크의 나사를 풀고 새 캐리어에 디스크를 삽입해야 합니다.

디스크 쌍 연결을 유지해야 합니다. 이전 어플라이언스의 슬롯 A1/A2에서 새 어플라이언스의 슬롯 B1/B2로 디스크 쌍을 배치할 수 있지만 디스크를 같은 슬롯에 함께 보관해야 합니다. 그렇지 않으면 Panorama가 데이터를 성공적으로 복원하지 못할 수 있습니다.

STEP 8 | M-시리즈 어플라이언스가 수집기 그룹의 일부인 경우 사용 중지된 M-시리즈 어플라이언스 일련번호가 여전히 올바른 수집기 그룹의 일부인지 확인합니다.

```
debug log-collector-group show name <Log CollectorGroup name>
```

 ©2024 Palo Alto Networks, Inc.

STEP 9 | 마이그레이션을 위해 디스크를 준비합니다.



각 디스크 쌍에 대한 메타데이터를 생성하면 인덱스가 다시 작성됩니다. 따라서 데이터 크기에 따라 이 프로세스를 완료하는 데 시간이 오래 걸릴 수 있습니다. 프로세스를 가속화하기 위해 여러 *CLI* 세션을 시작하고 각 세션에서 메타데이터 재생성 명령을 실행하여 모든 쌍에 대해 동시에 프로세스를 완료할 수 있습니다. 자세한 내용은 M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성을 참조하십시오.

1. 각 쌍에 대해 다음 CLI 명령을 실행하여 디스크 쌍을 활성화하십시오.

```
admin> request system raid add <slot> force no-format
```

예:

```
admin> request system raid add A1 force no-format
 admin> request system raid add A2 force no-format
```

force 및 **no-format** 인수가 필요합니다. **force** 인수는 디스크 쌍을 새 어플라이언스와 연결합니다. **no-format** 인수는 드라이브의 재포맷을 방지하고 디스크에 저장된 로그를 유지합니다.

2. 각 디스크 쌍에 대한 메타데이터를 생성합니다.



디스크의 로그 데이터 양에 따라 이 단계를 완료하는 데 최대 *60*시간이 소요될 수 있습니다. 새 *M-Series* 어플라이언스는 *###* 상태여야 합니다. *Panorama*가 *## ###* 상태인 경우 할당된 로그 수집기 *ID*를 가져오는 데 문제가 발생할 수 있습니다.

새 *M-Series* 어플라이언스가 *### HA* 피어인 경우 현재 *### HA* 피어의 Panorama 웹 인터페이스에 로그인하고 ***Panorama >*** 고가용성 및 고가용성을 위해 로컬 ***Panorama*** 일시 중단을 선택합니다.

로그를 성공적으로 마이그레이션한 후 고가용성을 위해 로컬 ***Panorama*** 기능을 설정합니다.

```
admin> request metadata-regenerate slot <slot_number>
```

예:

```
admin> request metadata-regenerate slot 1
```

 ©2024 Palo Alto Networks, Inc.

STEP 10 | 새 M-시리즈 어플라이언스에서 로컬 로그 수집기를 구성합니다.

> 일련번호가 필요한 명령이 있는 모든 단계의 경우 전체 일련번호를 입력해야 합니다. *Tab* 키를 눌러도 부분 일련번호가 완성되지 않습니다.

이 시점에서 새 M-시리즈 어플라이언스에서 디스크를 활성화하지 마십시오. 로그를 성공적으로 마이그레이션하면 Panorama가 자동으로 디스크를 활성화합니다.

1. Panorama 웹 인터페이스를 사용하거나 다음 CLI 명령을 사용하여 로컬 로그 수집기를 관리형 수집기로 구성합니다.

```
admin> configure admin# set log-collector <log-collector_SN>
 deviceconfig system hostname <log-collector-hostname>
 admin# exit
```

2. 변경 사항을 Panorama에 커밋합니다. 아직 수집기 그룹에 변경 사항을 커밋하지 마십시오.

```
admin> configure admin# commit
```

3. 로컬 로그 수집기가 Panorama에 연결되어 있고 해당 디스크 쌍의 상태가 존재/사용 가능한지 확인합니다.

```
admin> show log-collector serial-number <log-collector_SN>
```

디스크 쌍은 복원 프로세스의 이 단계에서 비활성화된 것으로 표시됩니다.

STEP 11 | Collector Group에 디스크가 없는 Log Collector를 추가합니다.

> 이 시점부터 *Panorama* 및 *Log Collectors*에서 마이그레이션 프로세스를 완료하는 데 필요한 커밋만 수행합니다. 다른 변경 작업을 보류하십시오.

1. Panorama CLI에 액세스.
2. 디스크가 없는 로그 수집기를 수집기 그룹에 추가할 수 있도록 Panorama 제한 덮어쓰기: **request log-migration-set-start**
3. 덮어쓴 제한을 커밋합니다.

```
admin> configure admin# commit force
```

 ©2024 Palo Alto Networks, Inc.

STEP 12 | 로그를 마이그레이션합니다.

새 *M* 시리즈 어플라이언스는 로그 마이그레이션을 #### ## ## *HA* 피어여야 합니다. 새 *M-Series* 어플라이언스가 ### *HA* 피어인 경우 현재 ### *HA* 피어의 Panorama 웹 인터페이스에 로그인하고 ***Panorama*** **>** 고가용성 및 고가용성을 위해 로컬 ***Panorama*** 일시 중단을 선택합니다.

로그를 성공적으로 마이그레이션한 후 고가용성을 위해 로컬 ***Panorama*** 기능을 설정합니다.

1. Panorama CLI에 액세스.
2. Collector Group의 구성원으로 새 로컬 Log Collector를 추가하고 Panorama에 변경 사항을 커밋합니다.

```
admin# set log-collector-group <collector_group_name> logfwd-
setting collectors <SN_managed_collector> admin# commit
 admin# exit
```

구성에서 삭제하지 않았기 때문에 이전 로컬 로그 수집기가 구성원 목록에 계속 나타납니다.

3. 각 디스크 쌍에 대해 로그를 새 어플라이언스로 마이그레이션합니다.

로그 마이그레이션을 시작하기 전에 새 *Panorama*가 ### *HA* 상태인지 확인합니다. 이는 로그를 성공적으로 마이그레이션하는 데 필요합니다.

```
admin> request log-migration from <old_LC_serial_number> old-
disk-pair <log_disk_pair> to <new_LC_serial_number> new-disk-
pair <log_disk_pair>
```

예:

```
admin> request log-migration from 003001000010 old-disk-pair A
 to 00300100038 new-disk-pair A
```

4. Panorama에 변경 사항을 커밋합니다.

```
admin> configure admin# commit
```

 ©2024 Palo Alto Networks, Inc.

STEP 13 | 수집기 그룹을 재구성합니다.

1. 웹 인터페이스를 사용하여 로그를 포워딩하는 방화벽에 새 로그 수집기를 할당합니다(**Panorama** > 수집기 그룹 > 디바이스 로그 포워딩). 방화벽 기본 설정 목록에서 새 로그 수집기에 이전 로그 수집기와 동일한 우선 순위를 부여합니다.

   *CLI*를 사용하여 방화벽 기본 설정 목록의 우선 순위 할당을 변경할 수 없습니다.

2. 수집기 그룹에서 이전 로그 수집기를 삭제합니다.

   ```
   admin# delete log-collector-group <group_name> logfwd-setting
    collectors <old_LC_serial_number>
   ```

   예:

   ```
   admin# delete log-collector-group DC-Collector-Group logfwd-
   setting collectors 003001000010
   ```

3. Panorama 구성에서 이전 Log Collector를 삭제하고 Panorama에 변경 사항을 커밋합니다.

   ```
   admin# delete log-collector <old_LC_serial_number>
    admin# commit admin# exit
   ```

4. M-시리즈 어플라이언스 HA 피어의 구성을 동기화합니다.

   ```
   admin> request high-availability sync-to-remote running-config
   ```

5. 관리되는 방화벽이 새 로그 수집기로 로그를 보낼 수 있도록 수집기 그룹 변경 사항을 커밋합니다.

   ```
   admin> commit-all log-collector-config log-collector-
   group <collector_group_name>
   ```

   예:

   ```
   admin> commit-all log-collector-config log-collector-group DC-
   Collector-Group
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 14 | 새 로그 수집기에서 새 키를 생성합니다.

이 명령은 새 로그 수집기를 수집기 그룹에 추가하는 데 필요하며 교체할 로그 수집기의 수집기 그룹에 대해서만 실행해야 합니다. 이 단계에서는 기존 *RSA* 키를 삭제하고 *Panorama*에서 새 *RSA* 키를 생성할 수 있습니다.

1. Panorama CLI에 액세스합니다.
2. 새 로그 수집기에서 모든 RSA 키를 삭제합니다.

   request logdb update-collector-group-after-replacecollector-group <*collector-group-name*>

   프로세스를 완료하는 데 최대 10분이 소요될 수 있습니다.

STEP 15 | 수집기 그룹의 모든 로그 수집기에 대해 SearchEngine 상태가 활성인지 확인합니다.

수집기 그룹의 모든 로그 수집기에 대해 *SearchEngine* 상태가 활성이 될 때까지 계속하지 마십시오. 그러면 교체되는 로그 수집기에서 로그가 제거됩니다.

1. Panorama CLI에 액세스.
2. 다음 명령을 실행하여 로그 수집기 세부 정보를 표시합니다.
   - 모든 로그 수집기에 대한 Panorama:

     ## ### ## ##

     또는 각 전용 로그 수집기에서 다음 명령을 실행할 수 있습니다.

     ```
     show log-collector detail
     ```
3. SearchEngine 상태가 활성인지 확인합니다.

```
Redistribution status: none
```

```
Last commit-all: commit succeeded, current ring version 1
```

```
SearchEngine status: ####
```

```
md5sum 4e5055a359f7662fab8f8c4f57e24525 updated at 2017/06/14
 09:58:19
```

 ©2024 Palo Alto Networks, Inc.

STEP 16 | 새 로그 수집기에서 이전 로그 수집기 일련번호를 새 로그 수집기 일련번호로 바꿉니다.

이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체해야 새 Log Collector가 문제를 제거하기 위해 실행되지 않아 Log Collector가 필요할 때 마이그레이션된 로그에서 이전 데이터를 제거할 수 없습니다.

1. 로그 수집기 CLI에 액세스합니다.
2. 이전 Log Collector 일련번호를 새 Log Collector 일련번호로 교체합니다.

   request log-migration-update-logger from *<old-log-collector-serial-number>* to *<new-log-collector-serial-number>*

STEP 17 | ## ### Panorama HA 피어에 대한 HA 기능을 복원하여 보안 통신 재설정 상태를 보조 HA 피어로 강제 변경합니다.

1. 새(##) 파노라마 HA 피어의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 고가용성을 선택하고 로컬 **Panorama** 기능을 생성합니다.
3. 확인을 클릭하여 새 Panorama HA 피어에서 HA 기능 복원을 확인합니다.

STEP 18 | 새 Panorama HA 피어에서 관리 서버를 다시 시작합니다.

1. 새(##) 파노라마 HA 피어의 Panorama CLI에 로그인.
2. 관리 서버를 다시 시작하십시오.

```
admin> debug software restart process management-server
```

STEP 19 | (활성 기본 HA 피어의 RMA만 해당) Panorama HA 피어의 고가용성 구성을 복원합니다.

A/P HA 구성에서 ## HA 피어를 교체한 경우 이 단계를 건너뜁니다.

1. ## HA 피어의 Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 고가용성을 선택하고 일렉션(Election) 설정을 수정합니다.
3. 우선 순위에 대해 보조를 선택하고 확인을 클릭합니다.
4. 커밋 및 **Panorama**에 커밋을 선택합니다.
5. ## HA 피어의 Panorama 웹 인터페이스에 로그인.
6. **Panorama** > 고가용성을 선택하고 일렉션(Election) 설정을 수정합니다.
7. 우선 순위에 대해 기본을 선택하 고확인을 클릭합니다.
8. 커밋 및 **Panorama**에 커밋을 선택합니다.

비HA Panorama의 실패/RMA 후 로그 수집기 마이그레이션

고가용성(HA) 구성으로 배포되지 않은 Panorama 관리 서버에서 시스템 장애가 발생하면 이 절차를 사용하여 교체 Panorama에서 구성을 복원하고 관리하는 전용 로그 수집기의 로그에 대한 액세스를 복원합니다. 허용되는 마이그레이션 시나리오는 Panorama 관리 서버 모델에 따라 다릅니다.

오래된/실패한 **Panorama**	신규/교체 **Panorama**
Panorama 가상 어플라이언스	• Panorama 가상 어플라이언스

 ©2024 Palo Alto Networks, Inc.

오래된/실패한 **Panorama**	신규/교체 **Panorama**
	• M-200 어플라이언스 • M-500 어플라이언스 • M-600 어플라이언스
M-100 어플라이언스	• Panorama 가상 어플라이언스 • M-200 어플라이언스 • M-500 어플라이언스 • M-600 어플라이언스
M-500 어플라이언스	• Panorama 가상 어플라이언스 • M-200 어플라이언스 • M-500 어플라이언스 • M-600 어플라이언스

Panorama는 전용 로그 수집기가 로그를 저장하는 데 사용하는 세그먼트와 파티션을 매핑하는 링 파일을 유지 관리합니다. Panorama 모드의 M 시리즈 어플라이언스는 내부 SSD에 링 파일을 저장합니다. Panorama 가상 어플라이언스는 내부 디스크에 링 파일을 저장합니다. 시스템 장애가 발생하면 non-HA Panorama는 링 파일을 자동으로 복구할 수 없습니다. 따라서 Panorama를 교체할 때 전용 로그 수집기의 로그에 액세스하려면 링 파일을 복원해야 합니다.

이 절차를 수행하려면 시스템 오류가 발생하기 전에 Panorama 구성을 백업하고 내보내야 합니다.

*Palo Alto Networks*는 *HA* 구성에서 *Panorama*를 배포할 것을 권장합니다. 활성 *Panorama* 피어는 링 파일을 *HA* 구성의 수동 피어와 자동으로 동기화하므로 피어 중 하나를 교체해야 하는 경우에도 전용 로그 수집기의 로그에 대한 액세스를 유지합니다.

©2024 Palo Alto Networks, Inc.

STEP 1 | 새 Panorama 어플라이언스의 초기 설정을 수행합니다.

1. 필요에 따라 M 시리즈 어플라이언스를 설정하거나 Panorama 가상 어플라이언스를 설정합니다. 새 M 시리즈 어플라이언스를 설정하는 경우 새 M 시리즈 어플라이언스를 랙 마운트하는 방법에 대한 지침은 M 시리즈 어플라이언스 하드웨어 참조 안내서를 참조하십시오.
2. M 시리즈 어플라이언스의 초기 구성을 수행하거나 Panorama 가상 어플라이언스의 초기 구성을 수행합니다.

   이전 *M*-시리즈 어플라이언스가 *Panorama* 서비스에 대해 *MGT* 인터페이스 이외의 인터페이스(예: 로그 수집)를 사용한 경우 새 *M*-시리즈 어플라이언스(***Panorama*** > ***Setup*** > ***Interfaces***)의 초기 구성 중에 해당 인터페이스를 정의해야 합니다. *Panorama* 가상 어플라이언스는 *MGT* 이외의 인터페이스를 지원하지 않습니다.
3. Panorama를 등록합니다.
4. 새 Panorama 어플라이언스가 이전 어플라이언스와 동일한 모델인 경우에만 다음과 같이 라이선스를 양도하십시오. 그렇지 않으면 새 라이선스를 구입해야 합니다.
   1. Palo Alto Networks 고객 지원 웹사이트에 로그인합니다.
   2. 자산 탭을 선택한 다음 스페어 링크를 클릭합니다.
   3. 새 M-시리즈 어플라이언스의 일련번호를 클릭합니다.
   4. 라이선스 전송을 클릭합니다.
   5. 이전 어플라이언스를 선택하고 제출을 클릭합니다.
5. Panorama 지원 라이선스 활성화.
6. 방화벽 관리 라이선스를 활성화합니다.
7. Panorama용 콘텐츠 및 소프트웨어 업데이트 설치.

   M-500 어플라이언스에는 *Panorama 7.0* 이상의 버전이 필요합니다. *M-200* 및 *M-600* 어플라이언스에는 *Panorama 8.1*이 필요합니다. 소프트웨어 버전에 대한 중요한 세부 정보는 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | 이전 Panorama에서 교체 Panorama로 구성을 복원합니다.

1. 새 Panorama에 로그인하고 **Panorama** > 설정 > 작업을 선택합니다.
2. 명명된 **Panorama** 구성 스냅샷 가져오기를 클릭하고 백업 구성 파일 찾아보기를 클릭한 다음 확인을 클릭합니다.
3. 명명된 **Panorama** 구성 스냅샷 로드를 클릭하고 방금 불러온 파일의 이름을 선택한 다음 확인을 클릭합니다.

   *RMA Panorama*를 교체하려면 명명된 *Panorama* 구성 스냅숏을 로드할 때 규칙 ***UUID***를 유지해야 합니다. 이 옵션을 선택하지 않으면 *Panorama*는 구성 스냅숏에서 이전 규칙 *UUID*를 모두 제거하고 *Panorama*의 규칙에 새 *UUID*를 할당하므로 정책 규칙 적중 수와 같은 이전 *UUID*와 관련된 정보를 유지하지 않습니다.
4. 커밋 > **Panorama**에 커밋을 선택하고 변경 사항을 커밋합니다.
5. **Panorama** > 관리형 수집기를 선택한 다음 연결됨 열에 전용 로그 수집기에 대한 확인 표시가 표시되는지 확인합니다.

   전용 로그 수집기가 나타나지 않으면 다음 단계에 설명된 대로 수집기 그룹과 수집기 그룹을 다시 구성해야 합니다. 그렇지 않으면 전용 로그 수집기에 저장된 로그에 대한 액세스를 복원하기 위해 링 파일을 가져오는 다음 단계를 건너뜁니다.

 ©2024 Palo Alto Networks, Inc.

STEP 3 | Panorama에서 누락된 경우 전용 로그 수집기 및 수집기 그룹을 재구성합니다.

1. 전용 로그 수집기의 CLI에 액세스하고 다음 명령을 입력하여 수집기 그룹의 이름을 표시합니다.
   1. 다음 명령을 입력합니다.

      ```
      > request fetch ring from log-collector <serial_number>
      ```

      다음 오류가 표시됩니다.

      ```
      ## ##: # ### #### #####. <serial_number>
      ```

   2. 다음 명령을 입력합니다.

      ```
      > less mp-log ms.log
      ```

      다음 오류가 표시됩니다.

      ```
      Dec04 11:07:08 Error:
       pan_cms_convert_resp_ring_to_file(pan_ops_cms.c:3719): ## ##
      ## CA-Collector-Group ### #### ## ####.
      ```

      이 예에서 오류 메시지는 누락된 수집기 그룹의 이름이 CA-수집기-그룹임을 나타냅니다.
2. Collector Group을 구성하고 전용 로그 수집기를 할당합니다.

   ```
   > configure # set log-collector-group <collector-group-name>
    # set log-collector-group <collector-group-name> logfwd-
   setting collector <serial-number>
   ```

3. Panorama에는 변경 사항을 커밋하지만 Collector Group에는 커밋하지 마십시오.

   ```
   # commit # exit
   ```

 ©2024 Palo Alto Networks, Inc.

STEP 4 | 전용 로그 수집기에 저장된 로그에 대한 액세스를 복원하려면 링 파일을 가져옵니다.

1. 새 Panorama의 CLI에 액세스합니다.
2. 링 파일을 가져옵니다.

```
> request fetch ring from log-collector <serial-number>
```

예:

```
> request fetch ring from log-collector 123456789012
```



전용 로그 수집기의 일련번호를 모르는 경우 해당 *CLI*에 로그인하고 ***show system info operation*** 명령을 입력합니다.

3. 수집기 그룹에 변경 사항을 커밋합니다.

```
> commit-all log-collector-config log-collector-
group <collector-group-name>
```

M-시리즈 어플라이언스 RAID 쌍에 대한 메타데이터 재생성

M-700, M-600, M-500, M-300 또는 M-200 어플라이언스에서 시스템 장애가 발생하고 한 어플라이언스에서 다른 어플라이언스로 디스크를 물리적으로 이동해야 하는 경우 메타데이터를 재생성해야 합니다. 메타데이터는 디스크에서 로그를 찾는 데 필요합니다. 사용자가 로그 쿼리를 실행하면 쿼리는 이 메타데이터를 참조하여 요청된 로그 데이터에 액세스합니다.

M-시리즈 어플라이언스에 구성된 각 RAID 디스크 쌍에 대해 어플라이언스 CLI에 액세스하고 다음 명령을 실행하여 메타데이터를 재생성해야 합니다.

```
> request metadata-regenerate slot <slot_number>
```

예:

```
> request metadata-regenerate slot 1
```

RAID 디스크의 크기는 메타데이터 재생성에 걸리는 시간을 결정합니다. 평균적으로 100GB당 1시간이 걸립니다. 명령을 실행하면 명령이 완전히 실행될 때까지 CLI 세션이 잠깁니다. 여러 CLI 세션을 사용하여 시간을 절약할 수 있습니다. 예를 들어 1TB 드라이브의 RAID 쌍 4개를 총 4TB의 로그 데이터로 교체하려면 CLI 세션 4개를 시작하고 각 세션에서 명령을 실행하여 약 10시간 내에 모든 쌍/슬롯에 대한 메타데이터를 동시에 재생성합니다.

메타데이터 재생성 중에는 이러한 디스크가 속한 수집기 그룹을 사용할 수 없으며 로깅 또는 보고 작업(쓰기/쿼리)에 디스크 쌍을 사용할 수 없습니다. 그러나 새 방화벽 연결을 처리하거나 관리되는 방화벽에서 구성 변경을 관리하는 것과 같은 다른 작업을 수행할 수 있습니다. Panorama가 관리하고 이 RMA 프로세스의 일부가 아닌 다른 모든 수집기 그룹은 할당된 로깅 및 보고 기능을 정상적으로 수행할 수 있습니다.

 ©2024 Palo Alto Networks, Inc.

로그 쿼리 작업 보기

로그 쿼리 작업을 보고 로그 데이터 쿼리가 예상보다 오래 걸리는 이유를 조사하고 더 잘 이해할 수 있습니다. 시작하려면 먼저 Panorama에서 실행되는 모든 로그 쿼리 작업을 표시해야 합니다. 조사해야 하는 로그 쿼리 작업을 식별한 후 작업 ID를 사용하여 쿼리에 대한 자세한 정보를 보고 로그 쿼리에 문제가 발생한 이유를 더 잘 이해할 수 있습니다. Panorama에서 로그 데이터를 쿼리할 때 새 로그 쿼리 작업이 실행될 때 자세한 작업 ID 정보를 덮어씁니다.

STEP 1 | Panorama CLI에 로그인.

STEP 2 | Panorama에서 실행된 로그 쿼리 작업을 봅니다.

CLI 출력에는 jod ID, 쿼리가 실행된 시간, 쿼리 상태, 쿼리된 로그 데이터베이스, 쿼리된 로그 수, 실행되는 데 걸린 시간(ms)과 같이 실행된 각 로그 쿼리에 대한 일반 정보가 포함됩니다. 쿼리와 쿼리에 적용된 모든 필터를 실행한 관리자가 결과를 반환합니다.

```
admin@Panorama> show query jobs
```

```
admin@bingdot34> show query jobs

ID        Enqueue Time         State       Database  nlogs     Runtime(ms)    Us
er            Filter
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
42        2020/01/02 14:35:46  COMPLETE    threat    110       166.27         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))


41        2020/01/02 14:35:46  COMPLETE    system    110       163.84         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

40        2020/01/02 14:35:46  COMPLETE    config    110       158.23         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

39        2020/01/02 14:35:36  COMPLETE    config    110       162.58         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

38        2020/01/02 14:35:36  COMPLETE    system    110       172.68         ad
min           (((receive_time leq now)) and (receive_time in last-hour))

37        2020/01/02 14:35:36  COMPLETE    threat    110       188.80         ad
min           ((((receive_time leq 'now')) and (((subtype eq 'file')) or ((subty
pe eq 'data')))) and ((receive_time in 'last-hour')))
```

STEP 3 | 작업 ID를 사용하여 특정 작업에 대한 세부 정보 로그 쿼리 정보를 봅니다.

```
admin@Panorama> show query jobid <Job ID>
```

```
admin@bingdot34> show query jobid 42

Serial          ID        State     Num Req   Num Proc  RTT(Max)      Avg Recs/R
TTSoftware Ver    CG                                Last Update Time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
LOGDB           42        DONE      110       0         0.00      0.00
9.2.0           LOCAL                                 2020/01/02 14:35:46

PODABCD12       42        FAILED    110       0         0.00      0.00
9.2.0           PODABCD12                             2020/01/02 14:35:46
```

 ©2024 Palo Alto Networks, Inc.

RMA 방화벽 교체

RMA(Return Merchandise Authorization)와 관련된 관리 방화벽에서 구성을 복원하는 데 필요한 노력을 최소화하려면 Panorama에서 이전 방화벽의 일련번호를 새 방화벽의 일련번호로 바꾸십시오. 그런 다음 교체 방화벽에서 구성을 복원하려면 이전에 생성하고 방화벽에서 내보낸 방화벽 상태를 가져오거나 Panorama를 사용하여 PAN-OS 5.0 이상의 버전을 실행하는 관리 방화벽에 대한 부분 디바이스 상태를 생성하십시오. 일련번호를 교체하고 방화벽 상태를 가져오면 Panorama를 사용하여 방화벽을 다시 관리할 수 있습니다.

- 방화벽에 대한 부분적 디바이스 상태 생성
- RMA 방화벽 교체를 시작하기 전
- 교체 후 방화벽 구성 복원

방화벽에 대한 부분적 디바이스 상태 생성

Panorama를 사용하여 부분적인 디바이스 상태를 생성하면 LSVPN(Large Scale VPN) 설정에 대한 몇 가지 예외를 제외하고 관리되는 방화벽의 구성이 복제됩니다. 방화벽 구성의 두 가지 측면을 결합하여 부분적 디바이스 상태를 생성합니다.

- Panorama가 관리하는 중앙 집중식 구성 - Panorama는 방화벽에 푸시하는 공유 정책 규칙 및 템플릿의 스냅샷을 유지 관리합니다.
- 방화벽의 로컬 구성 - 방화벽에서 구성 변경을 커밋하면 로컬 구성 파일의 복사본이 Panorama로 전송됩니다. Panorama는 이 파일을 저장하고 이를 사용하여 부분 디바이스 상태 번들을 컴파일합니다.

> *LSVPN* 설정에서 *Panorama*에서 생성하는 부분 디바이스 상태 번들은 방화벽에서 내보내는 버전과 동일하지 않습니다(***Device*** > ***Setup*** > 작업을 선택한 다음 디바이스 상태 내보내기를 클릭). 디바이스 상태 내보내기를 수동으로 실행하거나 *XML API* 스크립트를 예약하여 파일을 원격 서버로 내보내는 경우 방화벽 교체 워크플로에서 내보낸 디바이스 상태를 사용할 수 있습니다.
>
> 디바이스 상태를 내보내지 않은 경우 교체 워크플로에서 생성하는 디바이스 상태에는 인증서 세부 정보 및 등록된 방화벽과 같은 동적 구성 정보가 포함되지 않으며, *LSVPN* 포털과 같은 방화벽 기능의 전체 구성을 복구하는 과정이 요구됩니다. 자세한 내용은RMA 방화벽 교체를 시작하기 전을 참조하십시오.

Panorama는 디바이스 상태를 저장하지 않습니다. 교체 후 방화벽 구성 복원에 나열된 CLI 명령을 사용하여 요청 시 생성합니다.

RMA 방화벽 교체를 시작하기 전

- ☐ 방화벽이 SD-WAN 클러스터에 속하는 경우 RMA가 있을 때 워크플로에 따라 SD-WAN 디바이스를 교체해야 합니다.
- ☐ 교체할 방화벽에는 PAN-OS 5.0.4 이상의 버전이 있어야 합니다. Panorama는 이전 PAN-OS 버전을 실행하는 방화벽에 대한 디바이스 상태를 생성할 수 없습니다.

©2024 Palo Alto Networks, Inc.

- ❑ 교체할 방화벽에 대한 다음 세부 정보를 기록합니다.
  - 일련번호 - 이전 방화벽에서 교체 방화벽으로 라이선스를 이전하려면 Palo Alto Networks 고객 지원 웹 사이트에 일련번호를 입력해야 합니다. 또한 Panorama에 이 정보를 입력하여 이전 일련번호에 대한 모든 참조를 교체 방화벽의 새 일련번호로 교체합니다.
  - (권장) **PAN-OS** 버전 및 콘텐츠 데이터베이스 버전 - URL 데이터베이스 공급업체를 포함하여 동일한 소프트웨어 및 콘텐츠 데이터베이스 버전을 설치하면 대체 방화벽에서 동일한 상태를 생성할 수 있습니다. 최신 버전의 콘텐츠 데이터베이스를 설치하기로 결정한 경우 데이터베이스에 대한 업데이트 및 추가로 인해 차이점을 발견할 수 있습니다. 방화벽에 설치된 버전을 확인하려면 Panorama에 저장된 방화벽 시스템 로그에 액세스하십시오.
- ❑ 배포를 위해 교체 방화벽을 준비합니다. 디바이스 상태 번들을 가져오고 구성을 복원하기 전에 다음을 수행해야 합니다.
  - 교체 방화벽이 이전 방화벽과 동일한 모델이고 유사한 작동 기능이 활성화되어 있는지 확인합니다. 다음 작동 기능을 고려하십시오. 교체 방화벽에 여러 가상 시스템이 있어야 하고, 점보 프레임 지원을 지원해야 합니까, 아니면 CC 또는 FIPS 모드에서 작동해야 합니까?
  - 네트워크 액세스를 구성하고 라이선스를 전송하고 적절한 PAN-OS 및 콘텐츠 데이터베이스 버전을 설치합니다.
- ❑ 이 방화벽 교체 프로세스를 완료하려면 Panorama CLI를 사용해야 하므로 관리자 계정에 운용 관리자 또는 Panorama 관리자 사용자 역할이 있어야 합니다.
- ❑ LSVPN 구성이 있고 위성 또는 LSVPN 포털로 배포된 Palo Alto Networks 방화벽을 교체하는 경우 Panorama에서 생성된 부분 디바이스 상태를 복원할 때 LSVPN 연결을 복원하는 데 필요한 동적 구성 정보를 사용할 수 없습니다. LSVPN 구성에서 방화벽에 대한 디바이스 상태를 자주 생성하고 내보내라는 권장 사항을 따랐다면 Panorama에서 생성하는 대신 방화벽 자체에서 이전에 내보낸 디바이스 상태를 사용하십시오.

  방화벽에서 디바이스 상태를 수동으로 내보내지 않고 Panorama에서 부분 디바이스 상태를 생성해야 하는 경우 누락된 동적 구성이 다음과 같이 방화벽 교체 프로세스에 영향을 줍니다.
  - 교체하려는 방화벽이 위성의 일련번호로 명시적으로 구성된 **GlobalProtect** 포털인 경우(**Network** > **GlobalProtect** > **Portals** > **Satellite** 구성), 방화벽 구성을 복원할 때 동적 구성이 손실되더라도 포털 방화벽은 위성을 성공적으로 인증할 수 있습니다. 인증에 성공하면 동적 구성 정보가 채워지고 LSVPN 연결이 복원됩니다.
  - 위성 방화벽을 교체하는 경우 포털에 연결 및 인증할 수 없습니다. 이 실패는 일련번호가 방화벽에 명시적으로 구성되지 않았기 때문에(**Network** > **GlobalProtect** > **Portals** > **Satellite** 구성) 또는 일련번호가 명시적으로 구성된 경우 교체된 방화벽의 일련번호가 이전 방화벽의 일련번호와 일치하지 않기 때문에 발생합니다. 디바이스 상태 번들을 가져온 후 연결을 복원하려면 위성 관리자가 방화벽에 로그인하고 포털 인증을 위한 자격 증명(사용자 이름 및 암호)을 입력해야 합니다. 인증 후 포털에서 LSVPN 연결에 필요한 동적 구성이 생성됩니다.

  그러나 방화벽이 고가용성 구성으로 구성된 경우 구성을 복원한 후 방화벽은 실행 중인 구성을 피어와 자동으로 동기화하고 원활하게 작동하는 데 필요한 최신 동적 구성을 얻습니다.

교체 후 방화벽 구성 복원

새 방화벽에서 방화벽 구성을 복원하려면 먼저 작동 모드 설정을 하고, 이전 방화벽에 설치된 것과 일치하도록 PAN-OS 소프트웨어 및 콘텐츠 릴리스 버전 업그레이드를 포함하여 새 방화벽에서 초기 구성을 수행

 ©2024 Palo Alto Networks, Inc.

합니다. 그런 다음 Panorama에서 이전 방화벽의 디바이스 상태를 내보내고 새 방화벽으로 가져옵니다. 마지막으로 Panorama로 돌아가서 새 방화벽이 연결되었는지 확인한 다음 Panorama와 동기화합니다.

방화벽이 SD-WAN 클러스터에 속하는 경우 RMA가 있을 때 워크플로에 따라 SD-WAN 디바이스를 교체해야 합니다.

STEP 1 | 새 방화벽에서 초기 구성을 수행하고 네트워크 연결을 확인합니다.

직렬 포트 연결 또는 SSH(Secure Shell) 연결을 사용하여 IP 주소, DNS 서버 IP 주소를 추가하고 새 방화벽이 Palo Alto Networks 업데이트 서버에 액세스할 수 있는지 확인합니다.

STEP 2 | (선택 사항) 새 방화벽의 작동 모드를 이전 방화벽의 작동 모드와 일치하도록 설정합니다.

이 작업에는 직렬 포트 연결이 필요합니다.

1. 방화벽의 유지 관리 모드에 액세스하려면 다음 CLI 명령을 입력하십시오.

```
> debug system maintenance-mode
```

2. 작동 모드의 경우 기본 메뉴에서 **FIPS ## ##** 또는 **CCEAL 4 ## ##**을 선택합니다.

STEP 3 | 새 방화벽에서 라이선스를 검색합니다.

다음 명령을 입력하여 라이선스를 검색합니다.

```
> request license fetch
```

STEP 4 | (선택 사항) 새 방화벽의 작동 상태를 이전 방화벽의 작동 상태와 일치시킵니다. 예를 들어, 다중 가상 시스템 기능에 대해 활성화된 방화벽에 대해 다중 가상 시스템(multi-vsys) 기능을 활성화합니다.

방화벽 설정과 관련된 명령을 입력합니다.

```
> set system setting multi-vsys on > set system setting jumbo-frame
 on
```

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 새 방화벽에서 PAN-OS 버전을 업그레이드하십시오.

기존 방화벽에 설치된 것과 동일한 PAN-OS로 업그레이드해야 합니다. 콘텐츠 릴리스 버전을 이전 방화벽에 설치된 것과 같거나 이후 버전으로 업그레이드해야 합니다.

다음 명령을 입력합니다.

1. 콘텐츠 릴리스 버전을 업그레이드하려면:

```
> request content upgrade download latest > request content
 upgrade install version latest
```

2. 안티바이러스 릴리스 버전을 업그레이드하려면:

```
> request anti-virus upgrade download latest > request anti-
virus upgrade install version latest
```

3. PAN-OS 소프트웨어 버전을 업그레이드하려면:

```
> request system software download version <version> > request
 system software install version <version>
```

STEP 6 | Panorama CLI로 이동하고 SCP(Secure Copy) 또는 TFTP를 사용하여 이전 방화벽의 디바이스 상태 번들을 컴퓨터로 내보냅니다(웹 인터페이스에서는 이 작업을 수행할 수 없음).

방화벽에서 디바이스 상태를 수동으로 내보낸 경우 이 단계를 건너뛸 수 있습니다.

내보내기 명령은 디바이스 상태 번들을 tar 압축 파일로 생성하고 지정된 위치로 내보냅니다. 이 디바이스 상태에는 LSVPN 동적 구성(위성 정보 및 인증서 세부 정보)이 포함되지 않습니다.

다음 명령 중 하나를 입력합니다.

```
> scp export device-state device <old serial#> to <login>
 @ <serverIP>: <path>
```

또는

```
> tftp export device-state device <old serial#> to <serverIP>
```

 ©2024 Palo Alto Networks, Inc.

STEP 7 | Panorama에서 이전 방화벽의 일련번호를 새 교체 방화벽의 일련번호로 교체합니다.

Panorama의 일련번호를 바꾸면 방화벽에서 구성을 복원한 후 새 방화벽이 Panorama에 연결할 수 있습니다.

1. 작동 모드에서 다음 명령을 입력하십시오.

```
> replace device old <old SN#> new <new SN#>
```

2. 구성 모드로 들어가 변경 사항을 커밋합니다.

```
> configure # commit
```

3. 구성 모드를 종료합니다.

```
# exit
```

 ©2024 Palo Alto Networks, Inc.

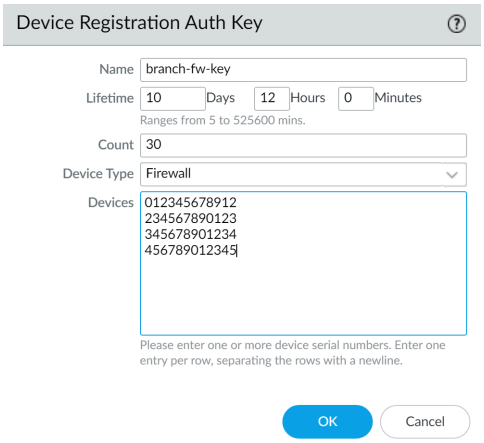
STEP 8 | (선택 사항) Panorama에서 디바이스 등록 인증 키를 생성합니다.

Panorama에 유효한 디바이스 등록 인증 키가 생성되지 않은 경우 이 단계가 필요합니다. Panorama에서 유효한 디바이스 등록 인증 키가 이미 생성된 경우 이 단계를 건너뜁니다.

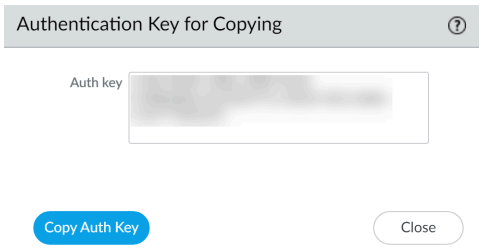
디바이스 상태 번들 내보내기는 방화벽을 *Panorama* 관리에 추가하는 데 사용된 디바이스 등록 인증 키를 내보내지 않습니다. 교체 후 방화벽 구성을 복원할 때 새 디바이스 등록 인증 키를 생성하여 새 방화벽을 *Panorama*에 추가해야 합니다.

1. Panorama 웹 인터페이스에 로그인.
2. **Panorama** > 디바이스 등록 인증 키를 선택하고 새 인증 키를 추가합니다.
3. 인증 키를 구성합니다.
   - 이름 - 인증 키를 설명하는 이름을 입력합니다.
   - 수명 - 새 방화벽을 온보딩하는 데 인증 키를 사용할 수 있는 기간을 지정하려면 키 수명을 입력합니다.
   - 개수 - 새 방화벽을 온보딩하는 데 인증 키를 사용할 수 있는 횟수를 지정합니다.
   - 디바이스 유형 - 인증 키가 방화벽을 인증하는 데 사용되도록 지정합니다.

     디바이스 등록 인증 키를 사용하여 방화벽과 로그 수집기를 모두 온보딩하려면 모두를 선택합니다.
   - (선택 사항) 디바이스 - 인증 키가 유효한 방화벽을 지정하기 위해 하나 이상의 디바이스 일련 번호를 입력합니다.
4. 확인을 클릭합니다.



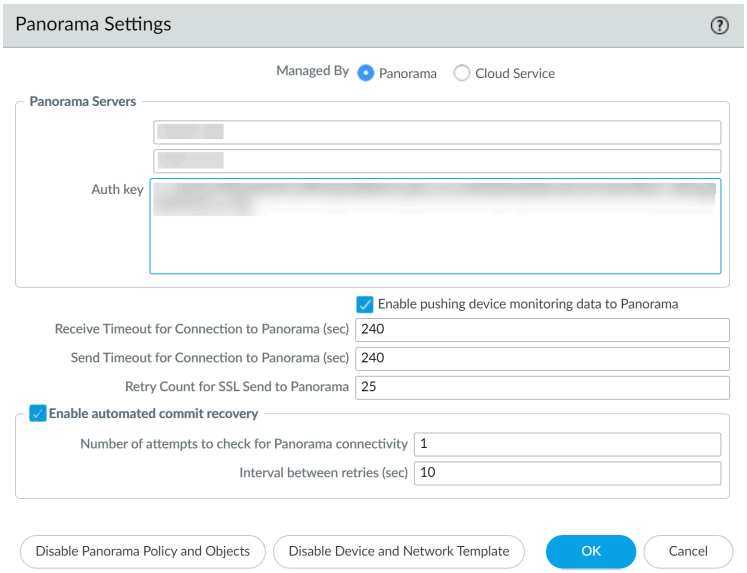
5. 인증 키를 복사하고 닫습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 9 | 새 방화벽에서 디바이스 상태를 가져오고 디바이스 등록 인증 키를 추가합니다.

1. 방화벽 웹 인터페이스에 로그인합니다.
2. 디바이스 > 설정 > 작업을 선택한 다음 구성 관리 섹션에서 디바이스 상태 가져오기 링크를 클릭합니다.
3. 파일을 찾아 확인을 클릭합니다.
4. 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.
5. Panorama에서 생성한 인증 키를 입력하고 확인을 클릭합니다.



6. 방화벽에서 실행 중인 구성에 대한 변경 사항을 커밋합니다.

STEP 10 | Panorama에서 방화벽 구성을 성공적으로 복원했는지 확인합니다.

1. Panorama 웹 인터페이스에 액세스하고 **Panorama** > 관리형 디바이스를 선택합니다.
2. 새 방화벽의 연결됨 열에 확인 표시가 있는지 확인합니다.

STEP 11 | 방화벽을 Panorama와 동기화합니다.

1. Panorama 웹 인터페이스에 액세스하고 커밋 > 커밋 및 푸시를 선택한 다음 푸시 범위에서 선택 사항을 편집합니다.
2. 디바이스 그룹을 선택한 다음 방화벽이 포함된 디바이스 그룹을 선택한 다음 디바이스 및 네트워크 템플릿 포함을 선택합니다.
3. 수집기 그룹을 선택한 다음 방화벽이 포함된 수집기 그룹을 선택합니다.
4. 확인을 클릭하여 푸시 범위에 대한 변경 사항을 저장합니다.
5. 변경 사항을 커밋하고 푸시합니다.

새 방화벽을 설치한 후 이전 방화벽이 계속 작동하던 기간 동안 보고서를 생성해야 하는 경우 *Panorama*에서 일련번호를 교체해도 로그의 정보를 덮어쓰지 않기 때문에 각 방화벽 일련번호에 대해 별도의 쿼리를 생성해야 합니다.

©2024 Palo Alto Networks, Inc.

커밋 실패 문제 해결

Panorama에서 커밋 또는 푸시 작업 실패가 발생하면 다음 조건을 확인합니다. 커밋 실패를 해결하려면 문제 해결 단계를 검토합니다.

증상	상태	해결
Panorama 커밋 문제	Panorama 커밋 잠금은 커밋에 성공한 후에도 해제되지 않습니다.	**Panorama** > 설정 > 관리를 선택하고 일반 설정을 편집하여 자동으로 커밋 잠금 획득 및 커밋을 비활성화합니다.
	다음 오류로 인해 Panorama 커밋이 실패합니다. `### dailytrsum #### 27MB# # ## ## #### 32MB## ####.`	**Panorama** > 설정 > 관리를 선택한 다음 로깅 및 보고 설정을 편집합니다. 일일 트래픽 요약, 일일 위협 요약, 주간 트래픽 요약 및 주간 위협 요약 로그 스토리지에 대한 `### %` 값을 35MB보다 큰 값으로 늘립니다. 또는 기본값 복원을 수행하십시오.
Panorama 푸시 문제	Panorama 관리 서버에는 관리하는 전용 로그 수집기 또는 방화벽보다 이전 소프트웨어 버전이 있습니다.	Panorama 관리 서버를 관리되는 방화벽, 로그 수집기, WildFire 어플라이언스 및 어플라이언스 클러스터와 같거나 더 높은 소프트웨어 버전으로 업그레이드하십시오. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조합니다.
	Panorama에서 템플릿 및 디바이스 그룹 구성 변경을 수신하는 기능은 방화벽에서 비활성화되어 있습니다.	방화벽 웹 인터페이스에 액세스하고 디바이스 > 설정을 선택한 다음, Panorama 설정을 편집하고 디바이스 및 네트워크 템플릿 활성화 및 **Panorama** 정책 및 개체 활성화를 클릭합니다.
	디바이스 등록 인증 키 문제로 인해 Panorama에서 관리형 방화벽으로의 구성 푸시가 실패합니다.	다음과 같은 경우 푸시 문제가 발생하는 관리형 방화벽에서 보안 연결 상태를 재설정하십시오. • 관리되는 디바이스가 이유 없이 Panorama에서 연결이 끊기고 다시 연결할 수 없습니다. • PAN-OS 10.1 이상 릴리즈를 실행하는 Panorama에서 PAN-OS 10.1 이상 릴리즈를 실행하는 다른

©2024 Palo Alto Networks, Inc.

증상	상태	해결
		Panorama로 방화벽 관리를 전환했습니다. • Panorama 또는 관리형 방화벽을 공장 기본 설정으로 재설정하고 관리형 방화벽을 다시 연결할 수 없습니다. 이 경우 Panorama에 대한 관리 디바이스 연결 복구을 수행해야 합니다.
	방화벽에 보류 중인 로컬 구성 변경으로 인해 Panorama의 구성 푸시가 실패합니다.	Panorama에서 디바이스로 푸시하거나 Panorama에서 **Panorama**에 커밋할 때 선택 항목을 편집하고 디바이스 후보 구성과 병합을 비활성화합니다.

- Panorama에서 커밋 문제 분류
- 템플릿 또는 디바이스 그룹 푸시 실패 문제 해결
- 보류 중인 로컬 방화벽 변경으로 인한 Panorama 푸시 실패 문제 해결

Panorama에서 커밋 문제 분류

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Panorama	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스

Panorama 관리 서버에서 커밋 문제를 분류하여 커밋이 실패한 이유를 식별합니다.

STEP 1 | PAN-OS 릴리즈 노트를 검토하여 커밋 실패의 원인이 될 수 있는 제한 사항, 기본 동작의 변경 사항 또는 알려진 문제를 확인합니다.

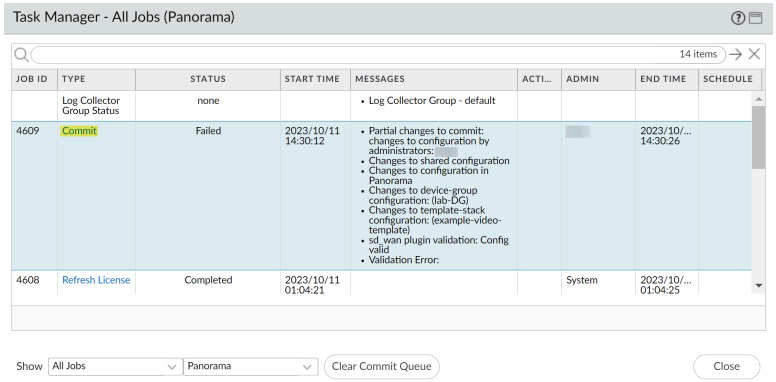
STEP 2 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

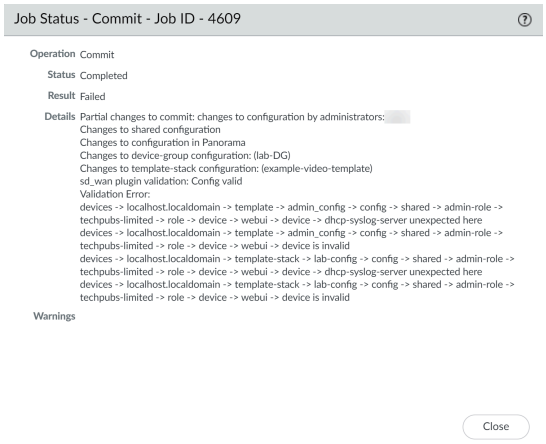
STEP 3 | Panorama 작업 관리자를 검토합니다.

1. 작업을 선택합니다.
2. 커밋 작업을 찾고 ## ID와 ## ##을 기록해 둡니다.

   ## 열에서 커밋을 클릭하여 작업 세부 정보를 확인합니다.



3. ### ## ##를 검토하여 커밋이 실패한 원인을 파악합니다. 이렇게 하면 Panorama 또는 방화벽 중 어디에서 커밋이 실패하는지 알아낼 수 있습니다.



 ©2024 Palo Alto Networks, Inc.

STEP 4 | PAN-OS 프로세스 및 프로세스 로그를 검토합니다.

1. Panorama CLI에 로그인.
2. 더 자세한 로그를 출력하려면 Panorama에서 디버그 로그를 활성화합니다.

```
admin> debug management-server
```

3. 관리 프로세스를 검토하여 성능이 저하된 ##가 있는지 확인합니다.

   이를 통해 어떤 관리 프로세스 로그가 커밋 실패에 영향을 미치는지 알 수 있습니다. ### 열에 별표(*)로 표시됩니다. ##### 열에는 구성 커밋과 관련된 다양한 관리 프로세스가 표시됩니다.

   문제가 나타나지 않으면 방화벽에서 커밋 실패가 발생한 것일 수 있습니다. 이 경우 방화벽 CLI에 이 명령을 입력해야 합니다.

```
admin> show management-clients
```

```
      Client PRI    State Progress
-------------------------------------------------------
    ha_agent  25     init        0
      sslmgr  10     init        0
       authd  10     init        0
     cryptod  10     init        0
      dagger  10     init        0   (op cmds only)
        cord  10     init        0
        logd  10     init        0
     reportd  10     init        0
     useridd  10     init        0
distributord  10     init        0
        iotd  10     init        0
```

4. Panorama 로그 파일을 검토하여 실패를 확인합니다.

   아래 명령에서 문제가 발생한 #####를 입력합니다.

```
admin> less mp-log <client>.log
```

   ## ##을 통해 커밋 실패를 일으킨 오류를 찾을 수 있습니다. 커밋이 실패한 이유는 ## ##로 표시됩니다.

5. 방화벽 CLI에 로그인하고 디바이스 서버 프로세스를 검토합니다.

```
admin> less mp-log devsrvr.log
```

   이 명령으로 방화벽의 구성 커밋 프로세스가 실패한 위치에 대한 추가 정보도 확인할 수 있습니다. 또한 외부 동적 목록(EDL)이 디바이스 메모리를 너무 많이 소비하는지 여부도 표시합니다.

템플릿 또는 디바이스 그룹 푸시 실패 문제 해결

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Panorama	☐ 디바이스 관리 라이선스 ☐ 지원 라이선스

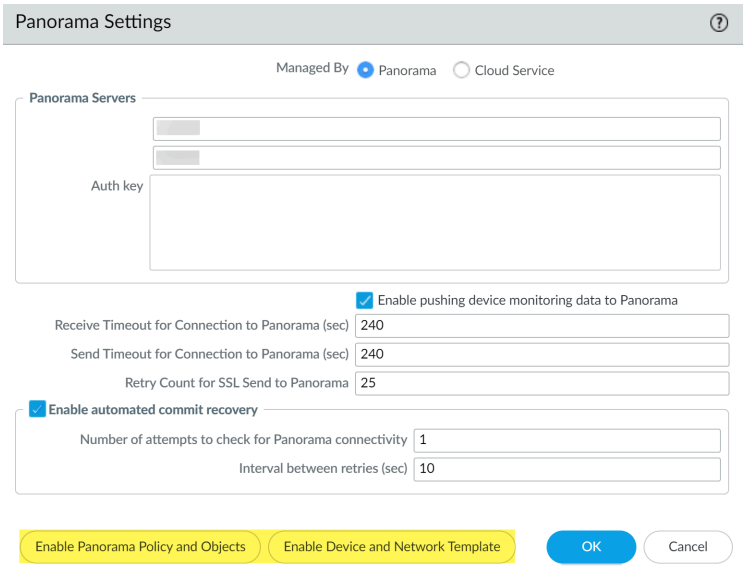
Panorama 관리 서버에서 템플릿 및 디바이스 그룹 구성 변경 사항을 수신하는 관리형 방화벽의 기능이 방화벽에서 비활성화되어 있는 문제를 해결합니다.

STEP 1 | 방화벽 웹 인터페이스에 로그인합니다.

STEP 2 | 디바이스 > 설정 > 관리를 선택하고 Panorama 설정을 편집합니다.

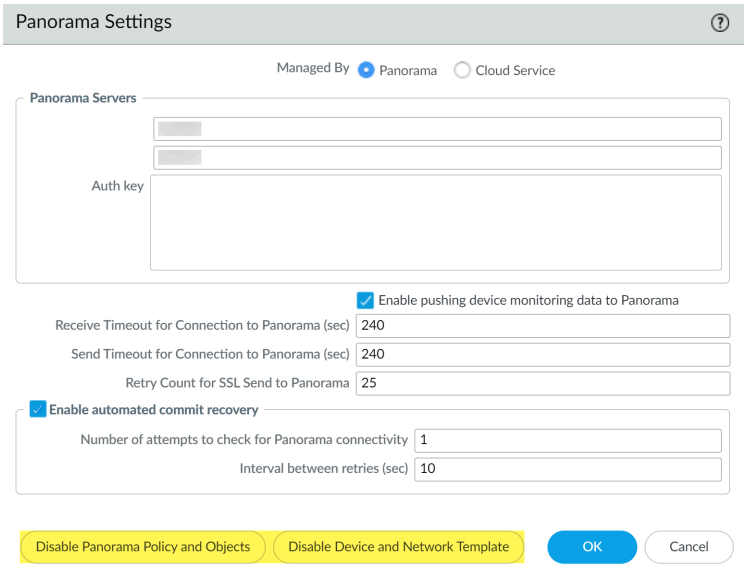
STEP 3 | Panorama ## # ##와 #### # #### ### 설정을 검토합니다.

아래 예는 Panorama로 푸시된 디바이스 그룹 및 템플릿 구성을 차단하도록 구성된 이러한 Panorama 설정을 보여줍니다.



STEP 4 | 각 설정을 클릭하여 Panorama에서 디바이스 그룹 및 템플릿 구성 푸시를 활성화합니다.

Panorama 정책 및 개체, 디바이스 및 네트워크 템플릿 설정을 활성화하라는 메시지가 표시되면 확인을 클릭합니다. 아래 예는 Panorama로 푸시된 디바이스 그룹 및 템플릿 구성을 허용하도록 구성된 이러한 Panorama 설정을 보여줍니다.



STEP 5 | Panorama 웹 인터페이스에 로그인하고 Panorama에서 구성 변경 사항을 푸시합니다.

 ©2024 Palo Alto Networks, Inc.

보류 중인 로컬 방화벽 변경으로 인한 Panorama 푸시 실패 문제 해결

어디에서 사용할 수 있습니까?	무엇이 필요합니까?
• Panorama	❑ 디바이스 관리 라이선스 ❑ 지원 라이선스

기본적으로 Panorama 관리에서 관리형 방화벽으로 구성을 푸시하면디바이스 후보 구성과 병합 설정이 활성화됩니다. 이 설정은 Panorama에서 푸시된 구성과 함께 방화벽에서 보류 중인 모든 로컬 구성 변경 사항을 커밋합니다. 로컬 구성이 변경된 경우 방화벽의 로컬 후보 구성이 불완전하거나 유효하지 않고 이 설정이 활성화되어 있으면 푸시가 실패할 수 있습니다.

관리형 방화벽에서 로컬 구성을 자주 변경하는 경우 이 설정을 비활성화하면 로컬 구성 변경 사항이 Panorama에서 푸시된 구성과 함께 커밋되는 것을 방지할 수 있습니다.

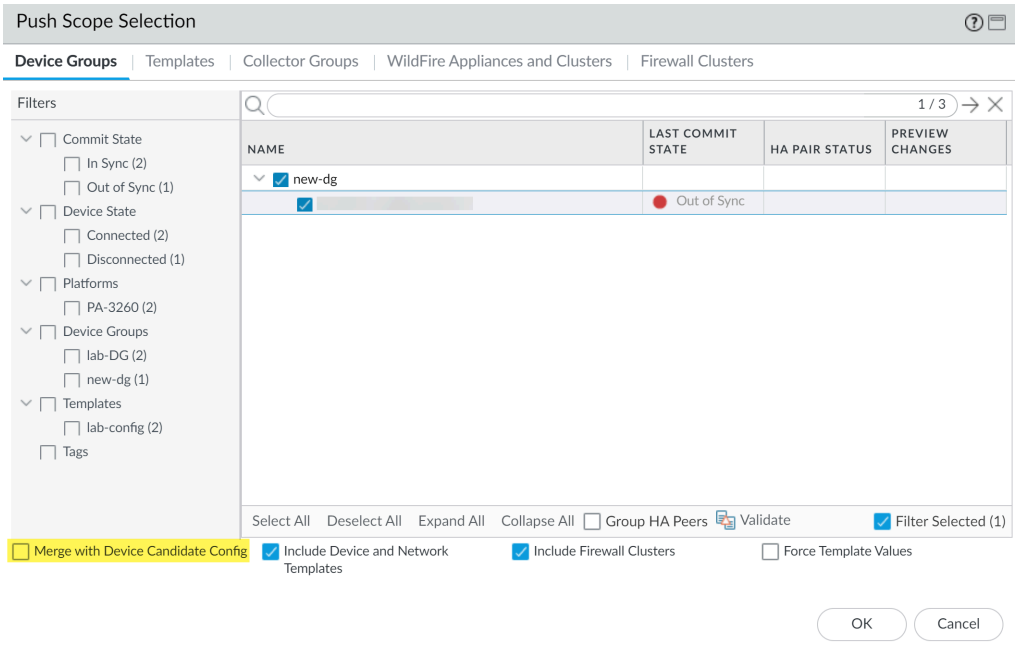
STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | 커밋 > 디바이스로 푸시 또는 커밋 및 푸시를 선택합니다.

STEP 3 | 선택 사항을 편집합니다.

STEP 4 | 디바이스 후보 구성과 병합을 선택 취소(비활성화)합니다.

STEP 5 | 확인을 클릭합니다.



STEP 6 | 푸시합니다.

©2024 Palo Alto Networks, Inc.

등록 또는 일련번호 오류 문제 해결

M-700, M-600, M-500, M-300 또는 M-200 어플라이언스에서 **Panorama** > 지원 페이지에 지원 라이선스 세부 정보가 표시되지 않거나 Panorama를 등록한 후에도 **Panorama** > 설정 > 관리 페이지에 일련번호에 대해 알 수 없음이 표시되면 다음 단계를 수행합니다.

STEP 1 | Panorama를 주문할 때 Palo Alto Networks에서 보낸 주문 이행 이메일에서 Panorama 일련번호를 기록해 두십시오.

STEP 2 | **Panorama** > 설정 > 관리를 선택한 다음 일반 설정을 편집합니다.

STEP 3 | 일련번호를 입력하고 확인을 클릭합니다.

STEP 4 | 커밋 > **Panorama**에 커밋을 선택한 다음 변경 사항을 커밋합니다.

 ©2024 Palo Alto Networks, Inc.

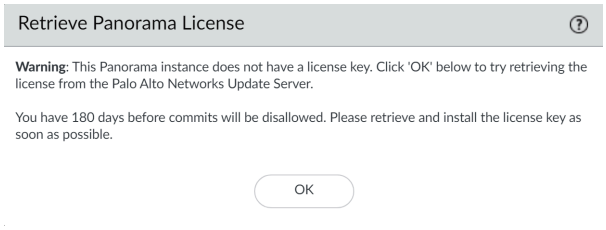
보고 오류 문제 해결

Panorama가 보고서를 생성하지 못하거나 보고서에 예상 데이터가 누락된 경우 해당 콘텐츠 버전(예: 애플리케이션 데이터베이스)은 관리형 수집기 및 방화벽의 콘텐츠 버전과 다를 수 있습니다. Panorama의 콘텐츠 버전은 관리형 수집기 및 방화벽의 콘텐츠 버전과 같거나 낮아야 합니다. 자세한 내용은 Panorama, 로그 수집기, 방화벽 및 WildFire 버전 호환성을 참조하십시오.

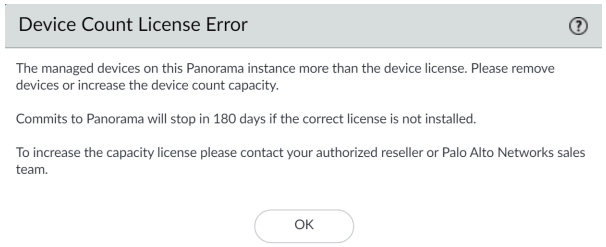
©2024 Palo Alto Networks, Inc.

디바이스 관리 라이선스 오류 문제 해결

PAN-OS 8.1로 업그레이드한 후 Panorama 가상 어플라이언스는 디바이스 관리 라이선스가 성공적으로 설치되었는지 확인합니다. 디바이스 관리 라이선스가 성공적으로 설치되지 않았거나 Panorama 가상 어플라이언스에서 관리하는 방화벽 수가 디바이스 관리 라이선스 제한을 초과하는 경우 유효한 디바이스 관리 라이선스를 설치할 수 있는 기간은 180일입니다. 유효한 디바이스 관리 라이선스가 설치되지 않은 경우 Panorama 웹 인터페이스에 로그인할 때마다 다음 경고가 나타납니다.



Panorama 가상 어플라이언스에서 관리하는 방화벽 수가 디바이스 관리 라이선스 제한을 초과하는 경우 Panorama 웹 인터페이스에 로그인할 때마다 다음 경고가 나타납니다.



이 문제를 해결하려면 유효한 어플라이언스 관리 라이선스를 설치하세요.

STEP 1 | 적절한 디바이스 관리 라이선스를 구입하려면 Palo Alto Networks 영업 담당자 또는 공인 대리점에 문의하십시오.

STEP 2 | Panorama 웹 인터페이스에 로그인합니다.

STEP 3 | Panorama 가상 어플라이언스가 온라인인지 오프라인인지에 따라 디바이스 관리 라이선스를 활성화/검색합니다.

- Panorama 가상 어플라이언스가 인터넷에 연결되어 있을 때 방화벽 관리 라이선스를 활성화/검색합니다.
- Panorama 가상 어플라이언스가 인터넷에 연결되어 있지 않을 때 방화벽 관리 라이선스를 활성화/검색합니다.

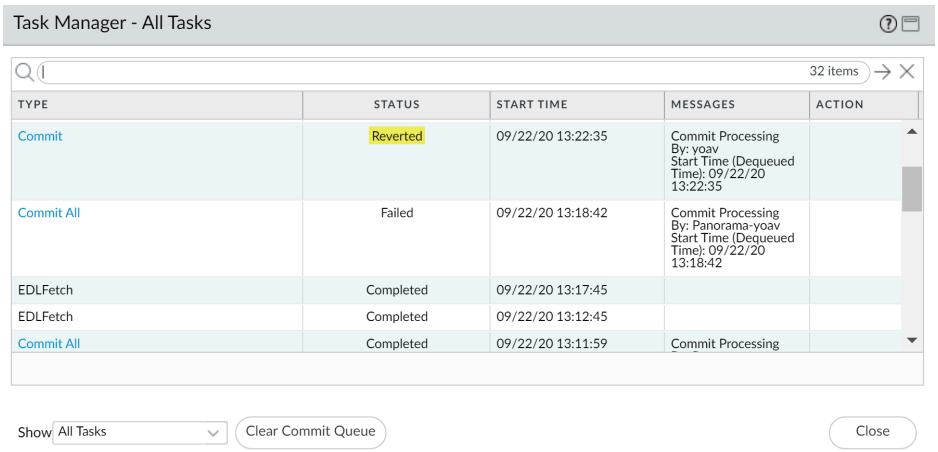
©2024 Palo Alto Networks, Inc.

자동으로 되돌린 방화벽 구성 문제 해결

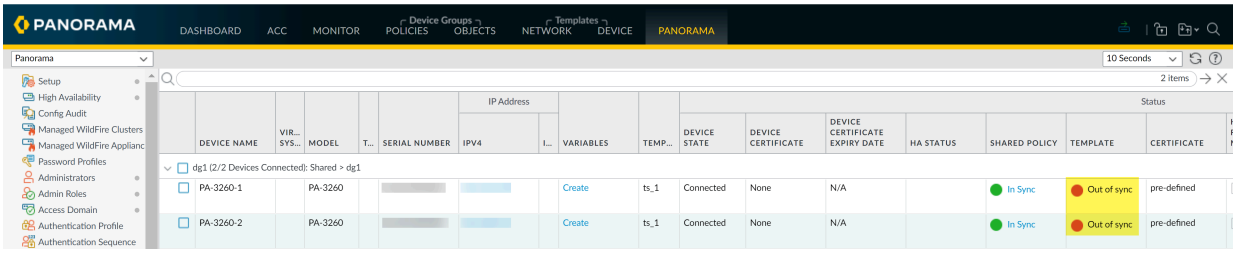
Panorama™ 관리 서버와 방화벽 사이의 연결이 끊어진 구성 변경으로 인해 관리 방화벽이 자동으로 구성을 되돌리는 경우 동기화되지 않은 방화벽 문제를 해결하여 변경 내용을 확인하고 마지막 구성 푸시의 어떤 측면에서 방화벽이 구성을 되돌렸는지 확인할 수 있습니다.

STEP 1 | 관리 방화벽이 자동으로 마지막 실행 구성으로 되돌아갔는지 확인합니다.

- 방화벽에서,
  1. 방화벽 웹 인터페이스를 시작합니다.
  2. 작업(웹 인터페이스의 오른쪽 하단 모서리)을 클릭합니다.
  3. 마지막 커밋 작업(Panorama에서 푸시되었거나 로컬에서 커밋됨)이 ### 상태를 표시하는지 확인합니다.



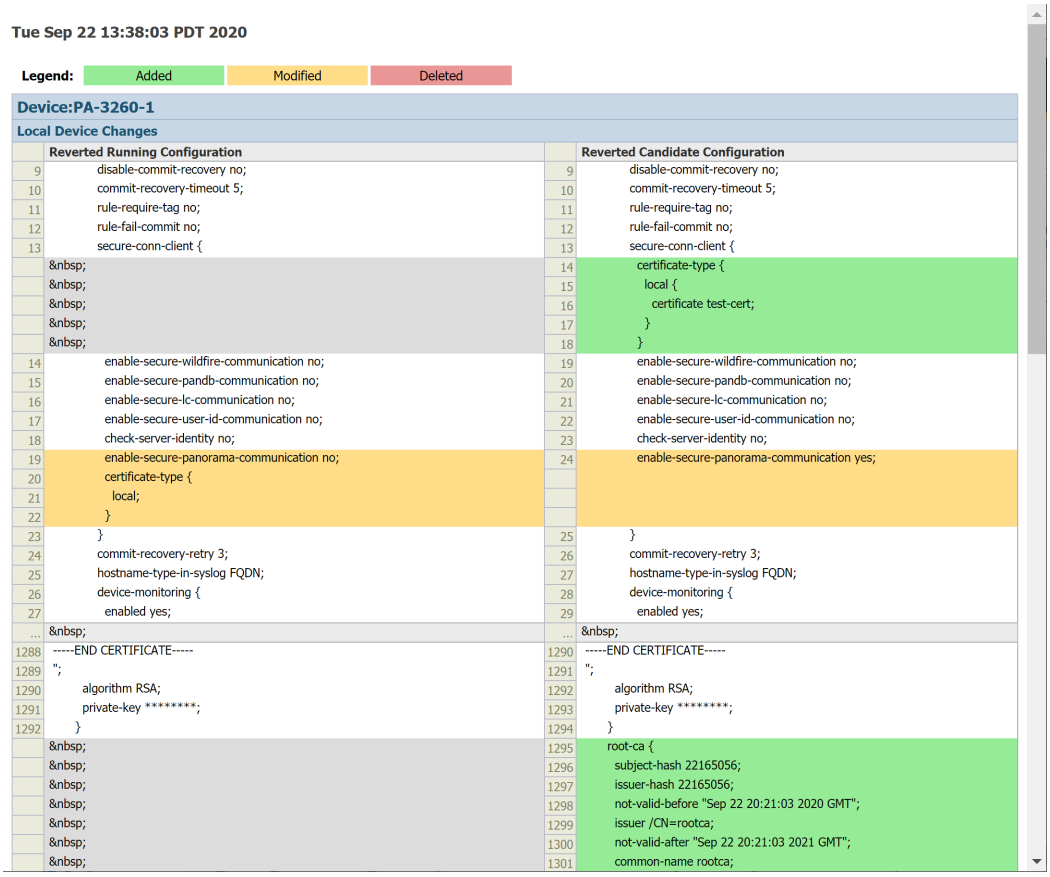
- Panorama에서,
  1. Panorama 웹 인터페이스에 로그인.
  2. **Panorama** > 관리되는 디바이스 > 요약을 선택합니다.
  3. 공유 정책 및 템플릿 동기화 상태를 봅니다. 최근에 Panorama에서 관리 방화벽으로 구성을 푸시하고 되돌린 경우 공유 정책 또는 템플릿이 ##### ##으로 표시됩니다(구성 변경 사항에 따라 다름).



STEP 2 | 관리 방화벽의 Last Merged Diff 열에서 **Show Last Merged Config Diff(**)를 선택하여 현재 실행 중인 구성과 되돌린 구성을 비교합니다. 이 예에서 Panorama에서 푸시된 정책 규칙은 관리되는

 ©2024 Palo Alto Networks, Inc.

방화벽과 Panorama 사이의 모든 트래픽을 거부하여 방화벽 구성이 자동으로 되돌아가도록 했습니다.



Tue Sep 22 13:38:03 PDT 2020

Legend: Added | Modified | Deleted

Device:PA-3260-1

Local Device Changes

	Reverted Running Configuration		Reverted Candidate Configuration
9	disable-commit-recovery no;	9	disable-commit-recovery no;
10	commit-recovery-timeout 5;	10	commit-recovery-timeout 5;
11	rule-require-tag no;	11	rule-require-tag no;
12	rule-fail-commit no;	12	rule-fail-commit no;
13	secure-conn-client {	13	secure-conn-client {
		14	certificate-type {
		15	local {
		16	certificate test-cert;
		17	}
		18	}
14	enable-secure-wildfire-communication no;	19	enable-secure-wildfire-communication no;
15	enable-secure-pandb-communication no;	20	enable-secure-pandb-communication no;
16	enable-secure-lc-communication no;	21	enable-secure-lc-communication no;
17	enable-secure-user-id-communication no;	22	enable-secure-user-id-communication no;
18	check-server-identity no;	23	check-server-identity no;
19	enable-secure-panorama-communication no;	24	enable-secure-panorama-communication yes;
20	certificate-type {		
21	local;		
22	}		
23	}	25	}
24	commit-recovery-retry 3;	26	commit-recovery-retry 3;
25	hostname-type-in-syslog FQDN;	27	hostname-type-in-syslog FQDN;
26	device-monitoring {	28	device-monitoring {
27	enabled yes;	29	enabled yes;
...		...	
1288	-----END CERTIFICATE-----	1290	-----END CERTIFICATE-----
1289	";	1291	";
1290	algorithm RSA;	1292	algorithm RSA;
1291	private-key ********;	1293	private-key ********;
1292	}	1294	}
		1295	root-ca {
		1296	subject-hash 22165056;
		1297	issuer-hash 22165056;
		1298	not-valid-before "Sep 22 20:21:03 2020 GMT";
		1299	issuer /CN=rootca;
		1300	not-valid-after "Sep 22 20:21:03 2021 GMT";
		1301	common-name rootca;

STEP 3 | 구성을 다시 푸시하기 전에 관리되는 방화벽과 Panorama 간의 연결을 끊지 않도록 필요에 따라 구성 개체를 수정합니다.

 ©2024 Palo Alto Networks, Inc.

작업 성공 또는 실패 상태 보기

Panorama 웹 인터페이스 의 오른쪽 하단에 있는 작업 관리자 아이콘을 클릭하여 Tasks 작업의 성공 또는 실패를 확인합니다. 작업 관리자는 문제를 디버깅하는 데 도움이 되는 자세한 메시지도 표시합니다. 자세한 내용은 Panorama 작업 관리자 사용을(를) 참조하십시오.

 ©2024 Palo Alto Networks, Inc.

관리되는 디바이스에 대한 정책 일치 및 연결 테스트

디바이스 그룹 및 템플릿 스택(template stack) 구성을 방화벽, 로그 수집기 및 WF-500 어플라이언스에 성공적으로 푸시한 후 올바른 트래픽이 관리 디바이스에 푸시된 정책 규칙과 일치하고 방화벽이 모든 적절한 네트워크 리소스에 성공적으로 연결할 수 있는지 테스트하십시오.

- 정책 규칙 트래픽 일치 문제 해결
- 네트워크 리소스에 대한 연결 문제 해결

정책 규칙 트래픽 일치 문제 해결

관리되는 방화벽에 대한 정책의 일치 관련 테스트를 수행하려면 관리되는 디바이스에 대한 정책 규칙 구성을 테스트하여 실행 중인 구성이 올바른 트래픽을 허용 및 거부하여 네트워크를 적절하게 보호하는지 확인하십시오. 구성된 규칙과 일치하는 트래픽에 대한 결과가 생성된 후 감사 목적으로 **PDF**로 내보내기 를 할 수 있습니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | **Panorama** > 관리형 디바이스 > 문제 해결을 선택하여 정책 일치를 수행합니다.



정책 탭에서 정책 일치 테스트를 실행할 수도 있습니다.

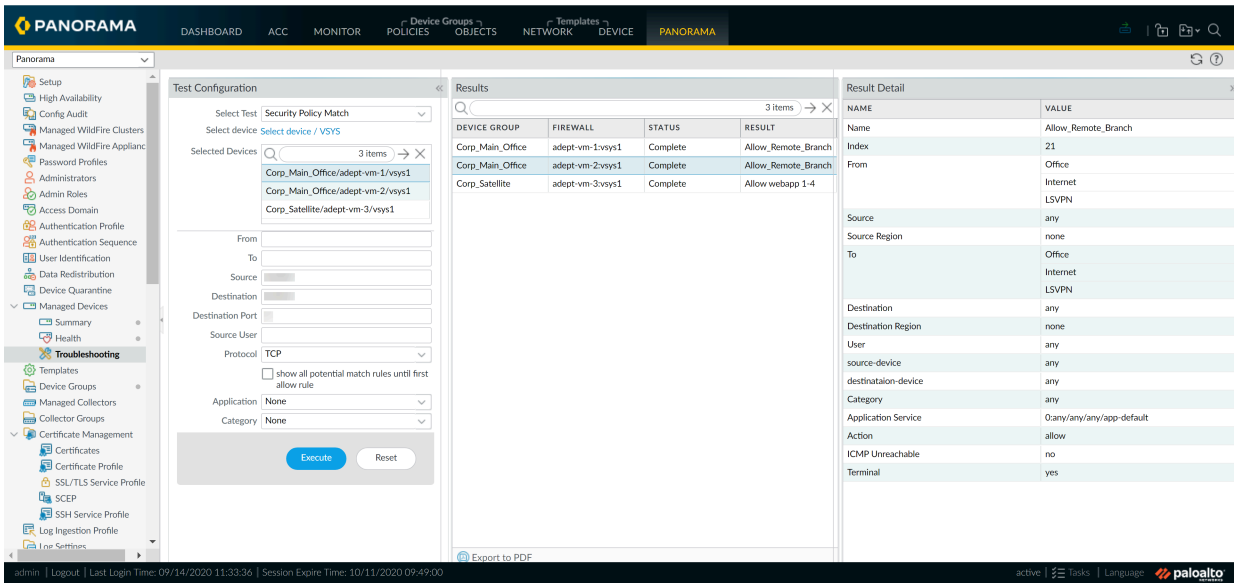
STEP 3 | 정책 일치 테스트를 수행하는 데 필요한 정보를 입력합니다. 이 예에서는 보안 정책 일치 테스트가 실행됩니다.

1. 테스트 선택 드롭다운에서 보안 정책 일치 선택합니다.
2. 디바이스**/VSYS**를 선택하고 테스트할 관리 방화벽을 선택합니다.
3. 트래픽이 발생한 소스 IP 주소를 입력합니다.
4. 트래픽에 대한 대상 디바이스의 대상 IP 주소를 입력합니다.
5. 트래픽에 사용되는 프로토콜 IP를 입력합니다.
6. 필요한 경우 보안 정책 규칙 테스트와 관련된 추가 정보를 입력합니다.

STEP 4 | 보안 정책 일치 테스트를 실행합니다.

 ©2024 Palo Alto Networks, Inc.

STEP 5 | 보안 정책 일치 결과를 선택하여 테스트 기준과 일치하는 정책 규칙을 검토합니다.



네트워크 리소스에 대한 연결 문제 해결

관리되는 방화벽에 대한 연결 테스트를 수행하여 관리되는 디바이스가 모든 적절한 네트워크 리소스에 연결할 수 있는지 확인합니다. 관리되는 디바이스에 대한 디바이스 구성을 테스트하여 실행 중인 구성이 관리되는 디바이스에 푸시된 구성이 여전히 해당 디바이스가 로그 수집기, 구성된 외부 동적 목록 및 Palo Alto Networks 업데이트 서버와 같은 리소스에 연결되는 것을 허용하는지 확인합니다. 또한 라우팅, WildFire®, Threat Vault, 핑(ping) 및 경로 추적 연결 테스트를 실행하여 Panorama™ 및 관리되는 디바이스가 네트워크 운영 및 보안에 중요한 외부 네트워크 리소스에 액세스할 수 있는지 확인할 수 있습니다. 결과가 생성된 후 감사 목적으로 **PDF**로 내보내기를 할 수 있습니다.

Ping 연결 테스트는 *PAN-OS 9.0* 이상의 버전을 실행하는 방화벽에 대해서만 지원됩니다.

STEP 1 | Panorama 웹 인터페이스에 로그인.

STEP 2 | **Panorama** > 관리형 디바이스 > 문제 해결을 선택하여 연결 테스트를 수행합니다.

정책 탭에서 정책 일치 테스트를 실행할 수도 있습니다.

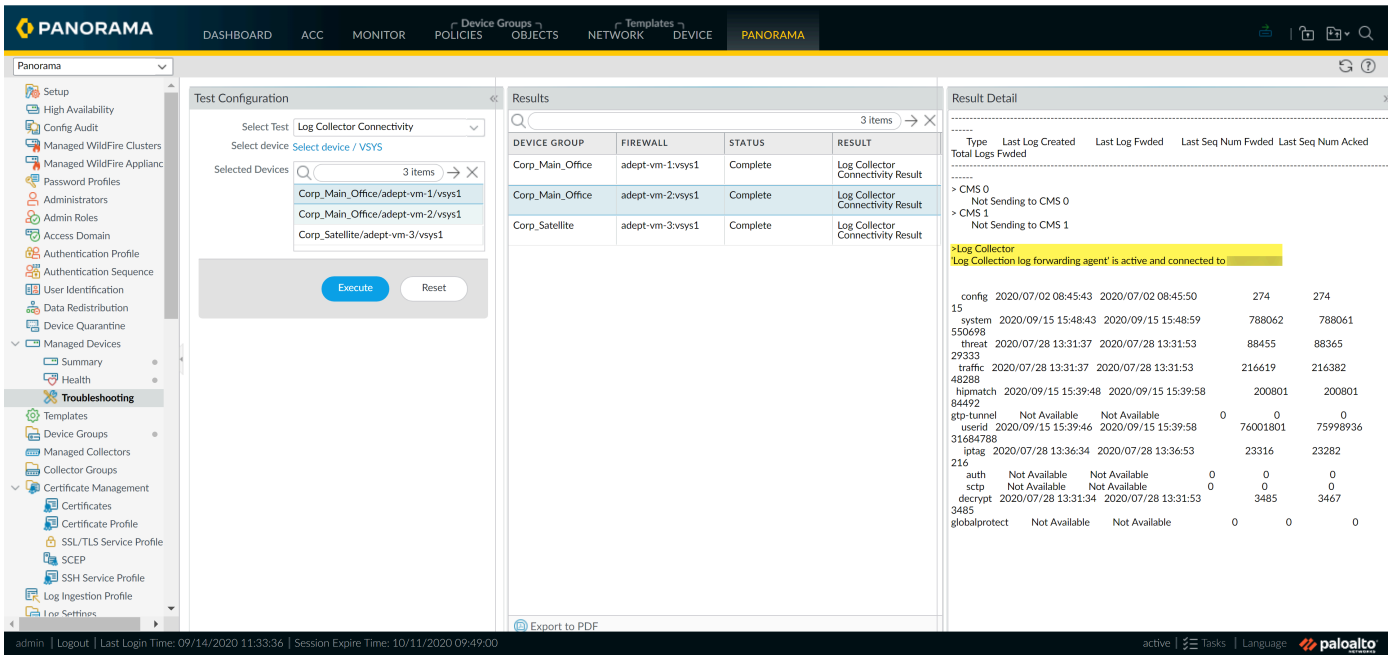
STEP 3 | 연결 테스트를 수행하는 데 필요한 정보를 입력합니다. 이 예에서는 로그 수집기 연결 테스트가 실행됩니다.

1. 테스트 선택 드롭다운에서 로그 수집기 연결을 선택합니다.
2. 디바이스**/VSYS**를 선택하고 테스트할 관리 방화벽을 선택합니다.
3. 필요한 경우 연결 테스트와 관련된 추가 정보를 입력합니다.

STEP 4 | 로그 수집기 연결 테스트를 실행합니다.

©2024 Palo Alto Networks, Inc.

STEP 5 | 로그 수집기 연결 결과를 선택하여 선택한 디바이스에 대한 로그 수집기 연결 상태를 검토합니다.



 ©2024 Palo Alto Networks, Inc.

관리되는 방화벽에 대한 통계 덤프 파일 생성

Panorama™ 관리 서버에서 관리하는 단일 방화벽 또는 Panorama에서 관리하는 모든 방화벽에 대해 지난 7일 동안의 네트워크 트래픽을 요약하는 일련의 XML 보고서를 생성합니다. 관리되는 방화벽을 선택한 다음 통계 덤프 파일을 생성한 후 통계 덤프 파일을 로컬로 디바이스에 다운로드할 수 있습니다.

Palo Alto Networks 또는 공인 파트너 시스템 엔지니어는 통계 덤프 파일을 사용하여 보안 수명 주기 검토(SLR)를 생성하고 관리형 방화벽을 성공적으로 배포한 후 보안 점검을 수행하여 보안 상태를 강화합니다. SLR은 네트워크에서 발견된 활동과 관련 비즈니스 또는 존재할 수 있는 보안 위험을 강조합니다. SLR에 대한 자세한 내용은 Palo Alto Networks 또는 공인 파트너 시스템 엔지니어에게 문의하십시오.

여러 관리 방화벽에 대한 통계 덤프 파일 생성을 완료하는 데 몇 시간이 걸릴 수 있습니다. 이 시간 동안 통계 덤프 파일 생성 사용자 인터페이스에서 탐색할 수 없으므로 *Panorama* 웹 인터페이스를 계속 사용할 수 있도록 *CLI*에서 통계 덤프 파일을 생성하는 것이 좋습니다.

*Palo Alto Networks*는 다음 명령을 사용하여 Panorama CLI에서 모든 관리 방화벽에 대한 통계 덤프 파일을 생성할 것을 권장합니다. 통계 덤프 파일을 성공적으로 내보내려면 *Panorama*가 *SCP* 또는 *TFTP* 서버에 연결할 수 있어야 합니다.

- ***SCP*** 서버

```
admin> scp export stats-dump to
 <username@hostname:SCP_export_path>
```

- ***TFTP*** 서버

```
admin> tftp export stats-dump to <tftp_host_address>
```

STEP 1 | Panorama 웹 인터페이스에 로그인.

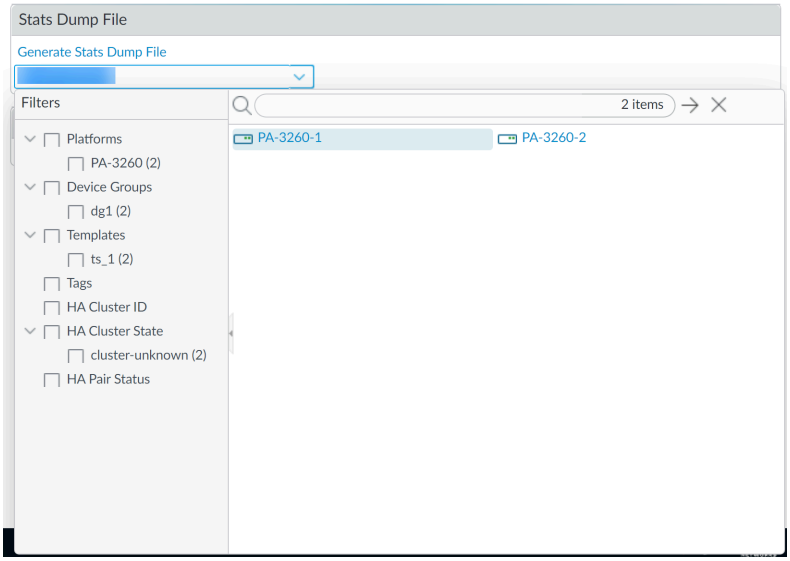
STEP 2 | **Panorama** > 지원을 선택한 다음 통계 덤프 파일로 이동합니다.

STEP 3 | 통계 덤프 파일을 생성할 관리 방화벽을 선택하십시오.

Panorama 웹 인터페이스에서 관리되는 단일 방화벽에 대한 통계 덤프 파일을 생성하는 것이 좋습니다.

관리되는 방화벽을 선택하지 않으면 기본적으로 모든 디바이스에 대한 통계 덤프 파일이 생성됩니다.

 ©2024 Palo Alto Networks, Inc.



STEP 4 | 통계 덤프 파일 생성.

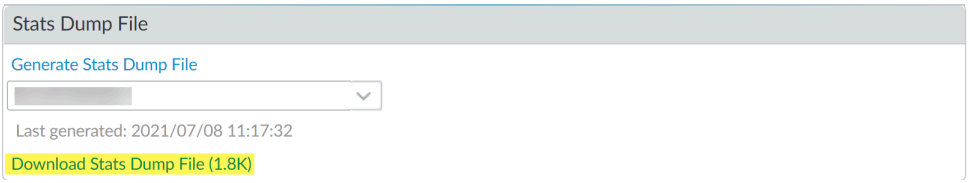
통계 덤프 파일 생성을 계속할지 묻는 메시지가 나타나면 예를 클릭합니다.

통계 덤프 파일 생성 상태의 진행률 표시줄이 표시됩니다.

단일 관리 방화벽의 경우 로그 데이터의 양에 따라 생성에 최대 1시간이 소요될 수 있습니다. 이 시간 동안 통계 덤프 파일 생성 상태 창에서 탐색할 수 없습니다.

STEP 5 | 통계 덤프 파일 다운로드를 클릭하여 통계 덤프 파일을 로컬 디바이스에 다운로드합니다.

다운로드한 통계 덤프 파일은 `tar.gz` 파일 형식입니다.



 ©2024 Palo Alto Networks, Inc.

Panorama에 대한 관리 디바이스 연결 복구

PAN-OS 10.1은 관리 방화벽, 전용 로그 수집기 및 WildFire 어플라이언스를 Panorama™ 관리 서버에 안전하게 온보딩하기 위한 디바이스 등록 인증 키를 도입했습니다. 아래 단계에서는 다음 시나리오에서 관리되는 디바이스 연결을 Panorama로 복구하는 방법을 설명합니다.

- 관리 대상 디바이스가 이유 없이 Panorama에서 연결이 끊기고 다시 연결할 수 없는 경우.
- PAN-OS 10.1 이상의 버전을 실행하는 Panorama에서 PAN-OS 10.1 이상의 버전을 실행하는 다른 Panorama로 방화벽 관리를 전환하려고 합니다.
- Panorama 또는 관리형 방화벽을 공장 기본 설정으로 재설정했지만 관리형 방화벽이 Panorama에 연결할 수 없는 경우.

Panorama에 대한 관리형 디바이스 연결 복구는 Panorama에 온보딩될 때 PAN-OS 10.1 이상을 실행하는 관리형 디바이스에만 적용됩니다. 설명된 동작은 PAN-OS 10.0 및 이전 릴리스를 실행하는 관리형 디바이스 또는 Panorama에서 이미 관리하는 동안 PAN-OS 10.1 이상으로 업그레이드된 관리형 디바이스에는 적용되지 않습니다.

다음 방화벽 플랫폼은 *Panorama*에 대한 설명된 연결 문제의 영향을 받지 않습니다.

- *ZTP*(제로 터치 프로비저닝)를 사용하여 *Panorama*에 온보딩된 관리형 방화벽.
- *CN* 시리즈 방화벽.
- *VMware NSX*에 배포된 관리형 방화벽.
- *VM* 시리즈 방화벽은 공개 하이퍼바이저 시장에서 구매합니다. 자세한 내용은 PAYG 방화벽을 참조하세요.

STEP 1 | 관리되는 디바이스의 보안 연결 상태를 재설정합니다.

1. 관리 디바이스 CLI에 로그인합니다.
   - 방화벽 CLI에 로그인합니다.
   - 전용 로그 수집기 CLI에 로그인합니다.
   - WildFire 어플라이언스 CLI에 로그인합니다.
2. 보안 연결 상태를 재설정합니다.

   이 명령은 관리되는 디바이스 연결을 재설정하고 되돌릴 수 없습니다.

   ```
   admin> request sc3 reset
   ```
3. 관리되는 디바이스에서 관리 서버를 다시 시작합니다.

   ```
   admin> debug software restart process management-server
   ```


©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama에서 관리형 디바이스의 보안 연결 상태를 지우고 새 디바이스 등록 인증 키를 생성합니다.

*Panorama*에서 관리되는 디바이스의 보안 연결 상태를 지우면 되돌릴 수 없습니다. 즉, 관리되는 디바이스의 연결이 끊기고 *Panorama*에 다시 추가해야 합니다.

1. Panorama CLI에 로그인.
2. Panorama에서 관리되는 디바이스의 보안 연결 상태를 재설정합니다.

   이 명령은 관리되는 디바이스 연결을 *Panorama*로 재설정하고 이 경우 다시 되돌릴 수 없습니다.

   ```
   admin> clear device-status deviceid <device_SN>
   ```

   여기서 **<device_SN>**은(는) 연결 상태를 지우려는 관리 대상 디바이스의 일련번호입니다.
3. Panorama에서 새 디바이스 등록 인증 키를 생성합니다.

   ```
   admin> request authkey add devtype <fw_or_lc) count
    <device_count> lifetime <key_lifetime> name <key_name> serial
    <device_SN>
   ```

   devtype 및 *##* 인수는 선택 사항입니다. 디바이스 유형이나 디바이스 일련번호와 관련이 없는 일반 사용 디바이스 등록 인증 키를 만들려면 이 두 인수를 생략하십시오.
4. 생성한 디바이스 등록 인증 키가 성공적으로 생성되었는지 확인합니다.

   ```
   admin> request authkey list *
   ```

   키 ##을 기록해 둡니다. 온보딩에 필요한 디바이스 등록 인증 키를 얻으려면 키 ##이 필요합니다.

   ```
   yoav@M-200(primary-active)> request authkey list *

   Name                                Cnt  Type     Expiry  Serial #
   ------------------------------------------------------------------------
   auth-key-fws                        100  fw       170470  1234567890,2345678901,3456789012,4567890123
   auth-key-lc                         100  lc       172852  0987654321,9876543210,8765432109,7654321098
   ```
5. 디바이스 등록 인증 # 값을 복사합니다.

   ```
   admin> request authkey list <key_name>
   ```

   ```
   yoav@M-200(primary-active)> request authkey list auth-key-fws

   Name       : auth-key-fws
     Count    : 100
     Type     : fw
     Lifetime : 169813s
     Key      : 2:_____:_____:_____
   ```

STEP 3 | 생성한 디바이스 등록 인증 키를 관리형 디바이스에 추가합니다.

1. 관리 디바이스 CLI에 로그인합니다.
   - 방화벽 CLI에 로그인합니다.
   - 전용 로그 수집기 CLI에 로그인합니다.
   - WildFire 어플라이언스 CLI에 로그인합니다.
2. 이전 단계에서 생성한 어플라이언스 등록 인증 키를 추가합니다.

   ```
   admin> request authkey set <auth_key>
   ```

   <auth_key>에 이전 단계에서 복사한 # 값을 입력합니다.

STEP 4 | Panorama에 대한 관리 디바이스 연결을 확인합니다.

```
admin> show panorama-status
```

Panorama 서버 ### 상태가 yes로 표시되는지 확인합니다.

이 절차로 관리 디바이스의 연결 문제가 해결되지 않으면 *Panorama*의 모든 관리 디바이스 연결을 완전히 재설정해야 할 수 있으므로 Palo Alto Networks 고객 지원에 추가 지원을 문의해야 합니다.

©2024 Palo Alto Networks, Inc.

만료된 디바이스 인증서 복원

Panorama™ 관리 서버, 전용 로그 수집기 또는 관리형 방화벽에 설치된 디바이스 인증서의 수명은 90일입니다. Panorama, 전용 로그 수집기 및 디바이스 인증서가 설치된 관리형 방화벽은 인증서가 만료되기 15일 전에 자동으로 디바이스 인증서 재설치를 시도합니다. 그러나 디바이스 인증서가 자동으로 다시 설치되지 않는 경우 수동으로 다시 설치할 수 있습니다.

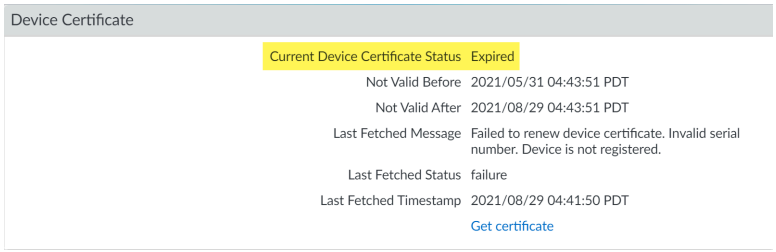
STEP 1 | Panorama 웹 인터페이스에 로그인.

 ©2024 Palo Alto Networks, Inc.

STEP 2 | Panorama, 전용 로그 수집기 및 관리형 방화벽에 대한 디바이스 인증서 상태를 검토합니다.

1. Panorama 디바이스 인증서 상태를 검토하려면 **Panorama** > 설정 > 관리를 선택하고 디바이스 인증서 섹션에서 ## #### ### ##를 확인합니다.

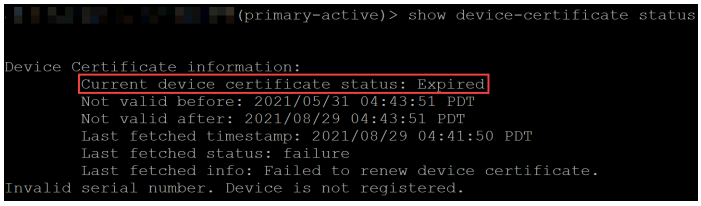
   ## #### ### ##에 ###이 표시됩니다.



2. 전용 로그 수집기 디바이스 인증서 상태를 검토하려면 전용 로그 수집기 CLI에 로그인하고 다음 명령을 입력하십시오.

```
admin>show device-certificate status
```

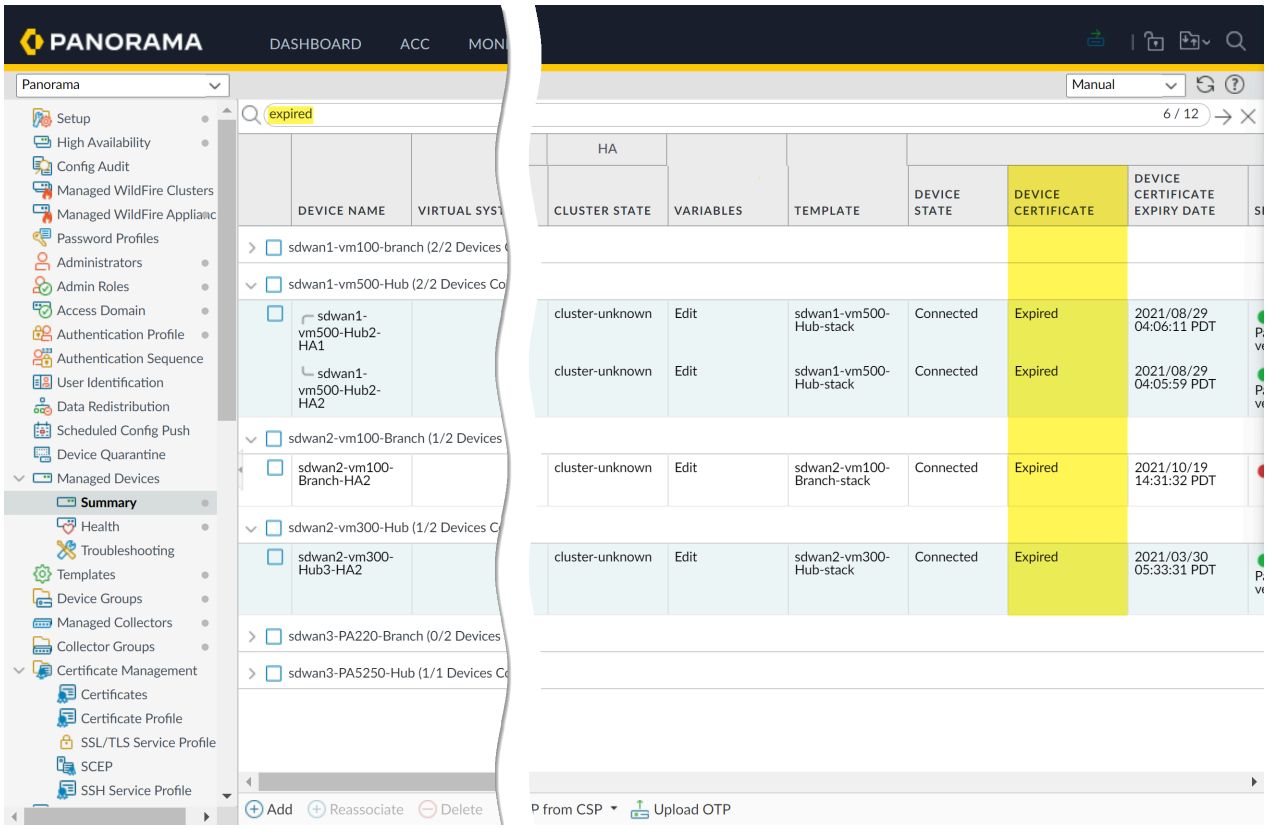
   ## #### ### ##에 ###이 표시됩니다.



3. 관리형 방화벽 디바이스 인증서 상태를 검토하려면 **Panorama** > 관리형 방화벽 > 요약을 선택하고 ###으로 필터링합니다.

   디바이스 인증서 열에 현재 ###인 디바이스 인증서 상태가 표시됩니다.

 ©2024 Palo Alto Networks, Inc.



STEP 3 | Panorama, 전용 로그 수집기 또는 관리형 방화벽에 만료된 디바이스 인증서를 다시 설치합니다.

> ***request certificate fetch otp<otp_value>*** 명령을 사용할 수 없다면 *Panorama*, 전용 로그 수집기 또는 관리형 방화벽이 신뢰할 수 있는 플랫폼 모듈*(TPM)* 디바이스인 것입니다.
>
> *TPM* 디바이스의 디바이스 인증서를 복원하려면 다음 명령을 실행합니다.
>
> ***request certificate fetch***

- Panorama 디바이스 인증서 설치
- 전용 로그 수집기에 대한 디바이스 인증서 설치
- 관리 방화벽에 대한 디바이스 인증서 설치

©2024 Palo Alto Networks, Inc.