

네트워크 장비의 구성 관리

NCM V12



NCM이 필요한 이유

NCM(Network Configuration Manager)은 라우터, 스위치, 방화벽 및 기타 네트워크 장치에서 구성과 규정 준수 등을 관리하고 변경하여 장치 구성 관리의 전체 수명주기를 제어 관리하는 도구입니다.

네트워크 장치를 점검 시 중요한 6가지 요소

구성 백업



구성 변경 관리



구성 템플릿(CONFIGLET)



규정 준수 관리



재난 관리



보고서



NCM으로 변경 관리를 하면

1. 모든 네트워크 구성 관리에 대해, 자동화, 백업, 규정 준수 점검으로 변경 관리의 프로세스를 간소화.
2. 자동 변경 추적을 통해 모든 구성 변경 기록을 유지.
3. 문제의 근본부터 식별하고 조사하고 수정하여 네트워크 문제를 해결
4. 우발적이고 악의적인 네트워크 장치 구성 변경으로 인한 네트워크 재해를 방지
5. 규정 준수를 구현하여 네트워크 장치의 다운타임을 줄이고 전반적인 보안을 보장

NCM에서 장치 파악 및 추가

다음 세 가지 방법 중 하나를 사용하여 NCM에서 장치가 파악될 수 있습니다.

장치 탐색, 수동 추가, 파일 가져 오기.

장치 탐색:

네트워크 장치의 IP 주소를 제공하여 장치를 탐색할 수 있습니다.

절차:

1. 설정-> 으로 이동
탐색 탭에서,
IP 주소와 IP 범위를 추가하면
장치가 추가됩니다.
장비 탐색 동안, CSV 파일 임포트
(가져 오기)로 장치를 추가할 수 있습니다.

Input	Credentials	Schedule
Discovery - Input		
Device Name/IP	IP Address	
	192.168.50.131	
IP Range	Netmask	
	255.255.255.0	
CSV File Import		

장치 추가 및 자격 증명(Credential) 적용

인벤토리에서 장치를 검색하고 추가하려면, 통신을 위한 SNMP 자격 증명을 지정해야 합니다.

Add Credential

- SNMP v1/v2**
Community for SNMP v1 and v2c devices
- SNMP v3**
Username and Password for monitoring v3 devices
- Telnet/SSH**
Username and Password for monitoring Linux and Solaris servers
- Windows/WMI**
Username and Password for monitoring Windows devices
- VMware**
Username and Password for monitoring VMware devices
- Citrix**
Username and Password for monitoring XenServers
- UCS**
Username and Password for monitoring UCS devices
- Storage**
Community or Username and Password for monitoring storage devices

Add Credential (SNMP v1/v2)

Name: test

Description: cred-1

Read Community:

Write Community:

SNMP Read:

Retype Password: public

SNMP Port: 161

SNMP Time Out (sec): 5

SNMP Retries: 0

Buttons: Back, Cancel, Save

Progress: Input (checked) - Credentials (active) - Schedule


Discovery - Credentials Add Credential

Name	Type	Description
Public	SNMP v1/v2	Default 'public' read community.
Simulator	SNMP v1/v2	v1/v2

Buttons: Back, Cancel, Next

수동 추가

장치를 추가하는 또 다른 방법은 인벤토리 탭의 오른쪽 상단의

 아이콘을 클릭하면, 사용자가 장치를 추가할 수 있도록 대화 상자가 열립니다.

Add Device

Hostname / IP Address

Vendor

Device Template Name

Series

Model

장비 추가에 필요한
호스트 명/IP 주소를 제공하십시오.

장비 목록 파일 가져 오기

장치의 호스트 명/IP 주소와 장치 템플릿 이름, 시리즈 및 모델을 알면 접근 인증을 제공하지 않고도 장치를 추가할 수 있습니다.

Add Device ✕

Choose Action: Add Device Import Devices from a Text File

File Location

Browse

Cancel Import

Note:

To import devices from a text file, ensure that the entries in the file are in the following format: (column names should be in the same order as shown in the format below with each name separated by a comma) Enter each entry in a new line.

Format

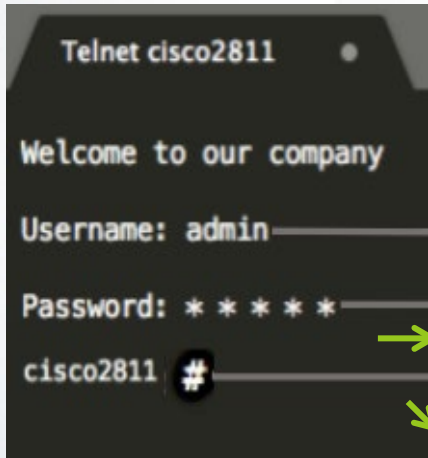
<Hostname/ IP Address>,<Device Template Name>,<Series>,<Model>

Example

```
catalyst2900.Cisco IOS Switch,2900,2924
192.168.111.11.Cisco IOS Router,800,805
192.168.111.22.Force10 E-Series Switch,E600
```

자격 증명 적용

자격 증명을 위해서
인벤토리에 장치를 추가한 후
구성이 필요한 모든 장치를 클릭



Apply Credentials

Options

Primary Additional

[New Profile](#)

Use Credential Profile: ---Select---

Login Name: ncm

Password:

Prompt: >

Enable UserName:

탐색 파악된 장치가 인벤토리에 추가된 직후 네트워크 장치 관리를 시작할 수 있습니다

Network Configuration Manager

License will expire in 20 days | Get Quote | Purchase | Request Demo

Dashboard | Inventory | Compliance | Alarms | Workflow | Reports | Settings

Inventory

Last 7 days

Not Backedup

1

Host Name	Device Type	Series	Model	Last Operation Status	Config Conflict	Compliance Status	Baseline Conflict
192.168.50...	Cisco Router	2800	2801	None	NA	[NA]	NA

Type | Credent... | Vendor | ...

Cisco IOS Router 1

Page 1 of 1 | 50 | View 1 - 1 of 1

구성 백업(Backup)

왜 백업이 필요합니까?

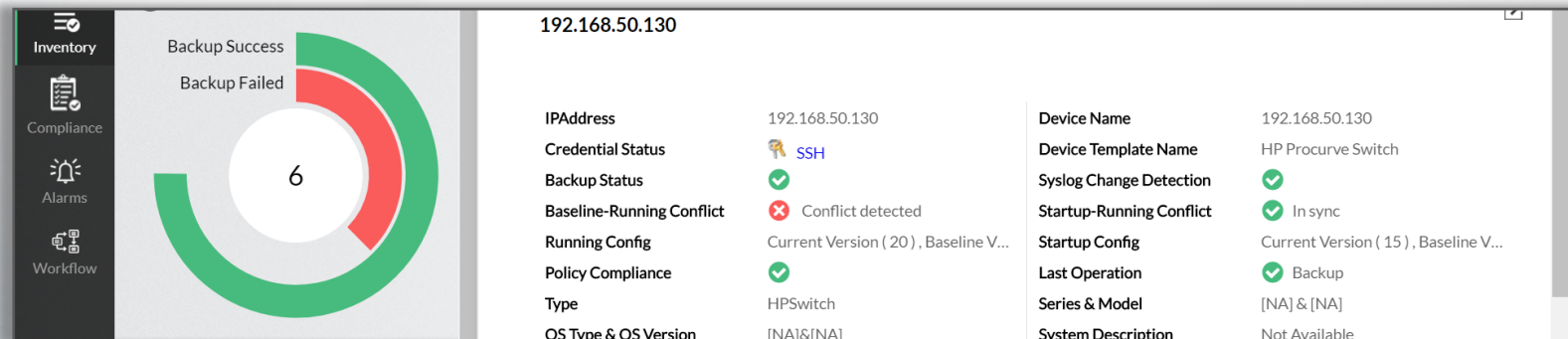
백업하면 다음에 도움이 됩니다.

- 비상 상태발생 시, 한 번의 클릭으로 네트워크 구성 복구
- 변경 발생 시, 자동으로 백업 구성
- 최신 변경에 기반한 구성 버전 관리와 안전한 저장

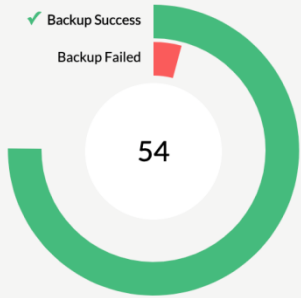
백업은 3가지 방법으로 수행할 수 있습니다.

- 수동 백업
- 예약 백업
- Syslog 기반 자동 백업

모든 구성의 백업 상태는 모든 백업 후에 업데이트됩니다.



즉각적인 구성 백업 & 대량 구성 백업



Type	Credent...	Vendor	Count
Cisco IOS Router			50
Cisco Modular Access Router			5
Juniper SRX			1
HP Procurve Switch			1

Network Configuration Manager

Dashboard | Inventory | Compliance | Change Management | Alarms | Tools | Settings | Reports | Support

Devices (57) | Groups (11) | Configs (138) | Changes (1155) | Drafts (10)

Host Name	IP Address	Device Type	Model	Last Operation Status	Config Conflict
192.168.49.6	192.168.49.6	Juniper SRX	srx50	Backup	In sync
192.168.50.131	192.168.50.131	Cisco Router	2801	Backup	Conflict detected
192.168.50.140	192.168.50.140	Cisco Router	CISCO2951-K9	Backup	Conflict detected
27.1.1.10	27.1.1.10	Cisco Router	2612	Backup	Conflict detected
27.1.1.11	27.1.1.11	Cisco Router	2612	Backup	Conflict detected
27.1.1.12	27.1.1.12	Cisco Router	2612	Backup	Conflict detected
27.1.1.13	27.1.1.13	Cisco Router	2612	Backup	Conflict detected
27.1.1.14	27.1.1.14	Cisco Router	2612	Backup	Conflict detected
27.1.1.15	27.1.1.15	Cisco Router	2612	Backup	Conflict detected
27.1.1.16	27.1.1.16	Cisco Router	2612	Backup	Conflict detected
27.1.1.17	27.1.1.17	Cisco Router	2612	Backup	Conflict detected
27.1.1.18	27.1.1.18	Cisco Router	2612	Backup	Conflict detected
27.1.1.19	27.1.1.19	Cisco Router	2612	Backup	Conflict detected
27.1.1.2	27.1.1.2	Cisco Router	2612	Backup	Conflict detected
27.1.1.20	27.1.1.20	Cisco Router	2612	Backup	Conflict detected
27.1.1.21	27.1.1.21	Cisco Router	2612	Backup	Conflict detected
27.1.1.22	27.1.1.22	Cisco Router	2612	Backup	Conflict detected
27.1.1.23	27.1.1.23	Cisco Router	2612	Backup	Conflict detected
27.1.1.24	27.1.1.24	Cisco Router	2612	Backup	Conflict detected
27.1.1.25	27.1.1.25	Cisco Router	2612	Backup	Conflict detected
27.1.1.26	27.1.1.26	Cisco Router	2612	Backup	Conflict detected

Recent 10 Backups

Host Name	Operation Status	Captured On
192.168.50.140	SUCCESS	Mar 27 2019 14:41:43 PM
192.168.50.131	SUCCESS	Mar 27 2019 14:38:32 PM
192.168.50.140	SUCCESS	Mar 27 2019 14:18:28 PM
27.1.1.45	SUCCESS	Mar 27 2019 13:02:01 PM

필요 시, 언제나 즉각적으로 원하는 수의 백업 수행.

매 백업마다 백업 상태를 성공/실패로 표시

네트워크 장치 간에 위험한 변경이 발생하는 경우 이 방법이 가장 적합

수동 및 Syslog 기반 자동 백업

수동 백업 :

장치를 선택하고 수동으로 장치를 백업합니다.

NCM

Enable Change Detection

Apply Credentials

Backup

Sync Configuration

Upload Config

Add Draft

Edit device details

Label Configuration

Update IP Address

Run Compliance Check

Stop Operation

Syslog 기반 자동 백업: 사용자가 장치 구성을 변경하면, 수행된 액션에 대한 syslog 알림이 수신되고, 백업이 자동으로 수행됩니다.

NCM

Enable Change Detection

Apply Credentials

Backup

Sync Configuration

Upload Config

Add Draft

Edit device details

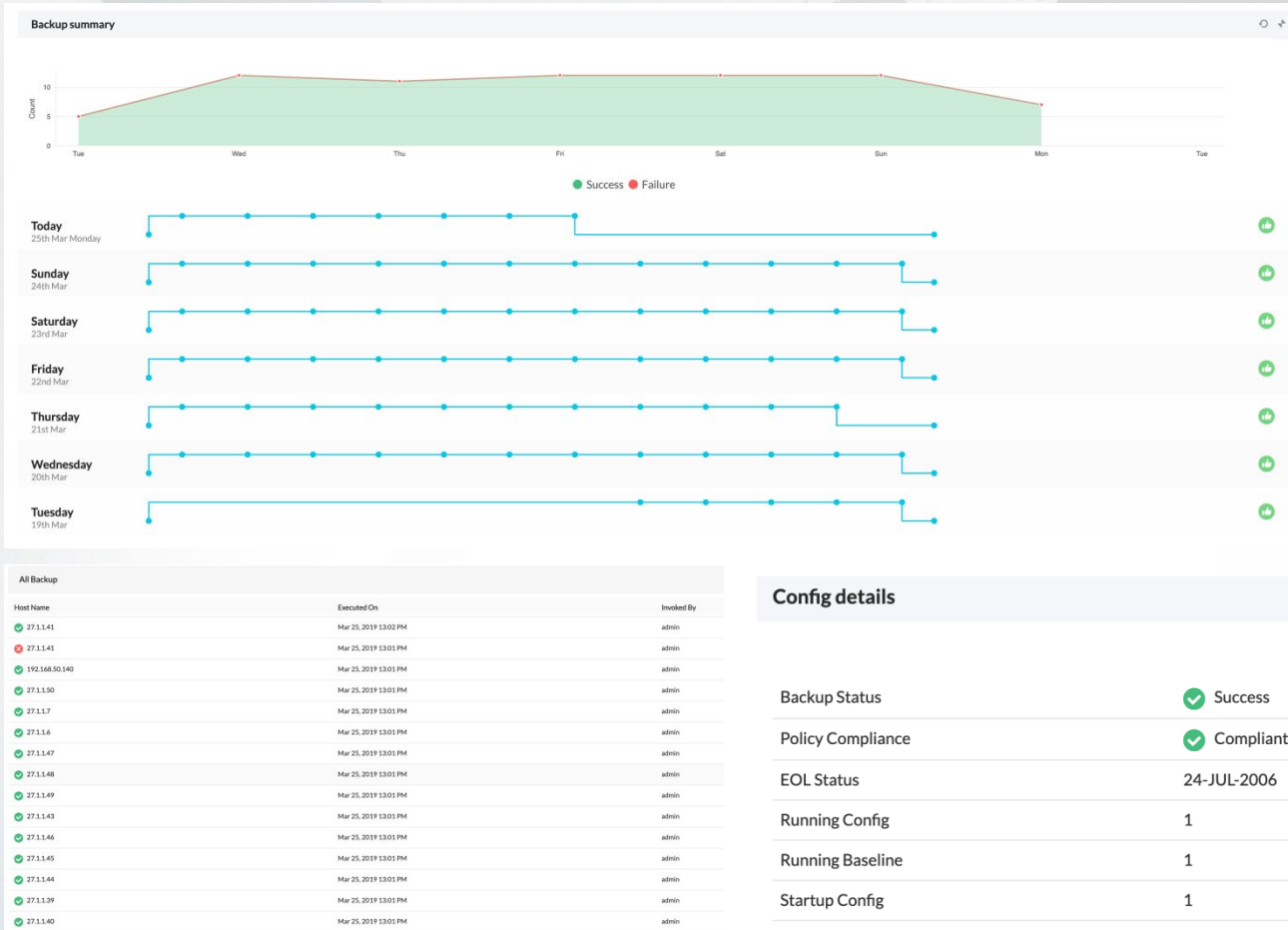
Label Configuration

Update IP Address

Run Compliance Check

Stop Operation

Syslog – 기반 자동 백업



장치에서 변경 감지를
활성화하여 백업 프로세스를
자동화

변경 사항에 대한 syslog 통지를
수신

변경 사항이 감지될 때마다 자동
구성 백업을 저장

예약 백업

- NCM은 예약된 백업을 제공하며, 여기서 백업 구성에 특정 시간을 설정할 수 있습니다
- 시간별, 일별, 주별, 월별 예약 백업 가능
- 지정된 시간에 자동으로 백업을 시작하고 이메일 통지를 보냅니다

Add Schedule

Select Specific Device Select Device Group

Available Devices

Search
192.168.49.6
192.168.49.7
192.168.49.101
192.168.50.130
192.168.50.131
192.168.50.140

Selected Devices

Search

Add Schedule

Send Email Notification

renu@gmail.com

(Use , for multiple address)

* Note :This report may contain personal identification data. Configured recipients will be receiving this report at the scheduled time. Please take extreme care while configuring the recipients.

Hourly

Daily

Weekly

Monthly

Once

Starts From

06-14-2018

Execute At

19

Hours

03

Minutes



Baseline 구성

기준 버전은 적용된 모든 구성 버전 중 최고 버전이며,

1. 예기치 않은 네트워크 중단 시, 그 기준 구성을 사용할 수 있습니다.
2. 최신 구성과 비교하여 변경 사항을 확인하고, 기준 구성과 다른 구성의 차이점을 확인하는 데 사용할 수 있습니다.

Device Name	192.168.50.131
Config Type	Running
Config Version	Version 87
Last Modified	Jun 12, 2018 09:24 PM
Owner	hema@zoho.com
Annotation	hematesting2

Diff with base-version

 0	 1	 0
Added	Modified	Deleted

구성 변경 관리

변경 관리의 중요성

자동화된 변경 추적은 네트워크에 대한 가시성을 높이고 네트워크 재난을 방지하는 데 중요합니다!



- 수동 변경 추적 제거
- 네트워크의 모든 변경 내용 보기
- 권한이 없는 사용자의 장치 액세스 제한
- 변경 통지 수신
- 결함 있는 변경 사항을 식별하여 신속하게 복원

실시간 변경 감지

REAL TIME CHANGE DETECTION(RTCD)

네트워크 장치의 구성을 변경하면 RTCD에 의해 해당 장치의 자동 백업이 트리거됩니다.

장점:

- 누가 변경했는지 통지를 받음.
- 변경된 시간과 날짜 파악
- 변경 사항이 저장된 후 즉시 구성 백업하여 안전성 보장

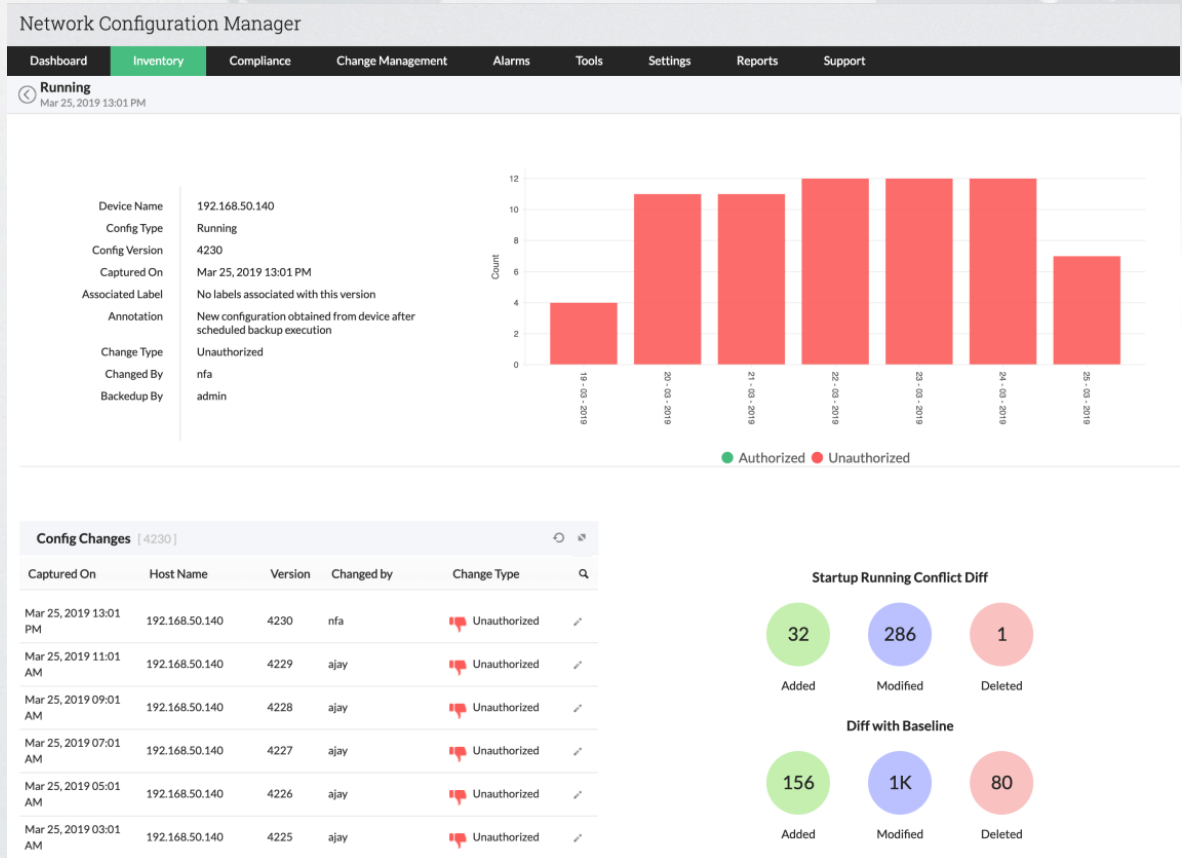
All Config Changes

Captured On	Host Name	IP Address	Changed By	Config Type
Jul 04, 2018 18:00 PM	192.168.50.140	192.168.50.140	mike1	Startup
Jul 04, 2018 18:00 PM	192.168.50.140	192.168.50.140	mike1	Running
Jul 04, 2018 17:36 PM	192.168.50.140	192.168.50.140	mike1	Running
Jul 04, 2018 17:25 PM	192.168.50.131	192.168.50.131	melab	Running
Jul 04, 2018 17:22 PM	192.168.50.131	192.168.50.131	melab	Startup
Jul 04, 2018 17:22 PM	192.168.50.131	192.168.50.131	melab	Running
Jul 04, 2018 17:01 PM	192.168.50.140	192.168.50.140	Not Available	Startup
Jul 04, 2018 17:01 PM	192.168.50.140	192.168.50.140	Not Available	Running
Jul 04, 2018 16:09 PM	192.168.50.131	192.168.50.131	nfa	Running



구성 변경 추적

Configuration Change Tracking



모든 네트워크 장치에서 구성 변경 추적을 자동화

구성 변경의 "무엇", "누구" 및 "언제"를 추적

필터를 적용하여 특정 장치에서 변경한 내용 보기 가능

중요 장치가 다운되기 전에 원치 않는 변경 사항을 복원.

“변경 감지 활성화” 작업

“변경 감지 활성화”가 지정된 경우

- NCM은 사용자가 로그인/로그아웃할 때 추적합니다.
- 변경 사항을 추적하고 사용자가 로그아웃한 후, 즉시 백업을 수행합니다.
- 백업을 현재 버전과 비교하고 변경 사항이 없으면 백업이 취소되고 변경 사항이 있으면 백업 내용이 데이터베이스에 저장됩니다.
- 사용자가 장치에서 수행하는 모든 작업에 대해 Syslog 메시지가 수신됩니다.

The screenshot shows the NCM interface with a sidebar on the left containing navigation icons for Dashboard, Inventory, Compliance, Alarms, and Workflow. The main area is titled 'Alarms' and 'Events' for IP 192.168.50.131. A large circular gauge displays '130 Alarms'. Below it, there are two smaller gauges for 'Critical' (130) and 'Trouble' (0). The main content area shows a list of events with columns for Message, Status, and Date/Time. A table of events is visible:

Message	Status	Date/Time
192.168.50.131 Configuration Changed by NCM User: admin.ncm at Jun 14, 2018 13:21 PM	Critical	14 Jun 2018 01:21:20 PM IST
192.168.50.131 Configuration Changed by ncm at Jun 13, 2018 16:36 PM	Critical	13 Jun 2018 04:36:35 PM IST
192.168.50.131 Configuration Changed by NCM User: hema@zoho.com at Jun 12, 2018 21:27 PM	Critical	12 Jun 2018 09:27:31 PM IST
192.168.50.131 Configuration Changed by ncm at Jun 11, 2018 16:09 PM		
192.168.50.131 Configuration Changed by ncm at Jun 11, 2018 16:09 PM		

The screenshot shows the 'Enable Change Detection' configuration window. It includes the following settings:

- Detecting Config Changes through Syslog: Enable Disable
- Syslog Server IP(s): 172.21.157.175
- Vendor Name: Cisco
- Logging Level: notifications

구성 비교

Network Configuration Manager

Dashboard Inventory Compliance Change Management Alarms Tools Settings Reports Support

Config Diff View

Added: (32) Modified: (286) Deleted: (1) Diff Only All Lines

LHS - Startup

- 79 flow exporter N/Aexporter
- 80 destination 172.24.148.31
- 81 transport udp 9996
- 82 template data timeout 60
- 83 custom application table timeout 60
- 457 flow-export destination 172.24.155.100 9996

RHS - Running

- flow exporter N/Aexporter
- destination 172.24.148.31
- transport udp 9996
- template data timeout 60
- custom application table timeout 60
- policy-map TestPolicy
- class class 0
- bandwidth 60
- flow-export destination 172.21.114.133 9996
- policy 302
- time-range 192.168.50.131 source-to 192.168.49.0/24
- request-data-size 24
- no 30
- server ConfigManager
- threshold 500
- timeout 0000
- ip sla schedule 302 ip sla forever aggrnt 60
- ip sla schedule 346 ip sla forever start-time 07:30:47 Jul 25 aggrnt 60
- ip sla schedule 374 ip sla forever start-time 04:46:46 Aug 12 aggrnt 60
- ip sla schedule 428 ip sla forever start-time 07:32:10 Jul 25 aggrnt 60
- ip sla schedule 9099 ip sla forever start-time 12:49:04 Aug 16
- ip sla schedule 9100 ip sla forever start-time 20:48:59 Aug 16 aggrnt 60
- ip sla schedule 9110 ip sla forever start-time 21:19:13 Aug 16
- ip sla schedule 9113 ip sla forever start-time 17:07:00 Aug 17
- ip sla schedule 9118 ip sla forever start-time 17:30:54 Aug 17
- ip sla schedule 9120 ip sla forever start-time 15:15:45 Aug 17 aggrnt 60
- ip sla schedule 9124 ip sla forever start-time 15:15:44 Aug 20
- ip sla schedule 9128 ip sla forever start-time 20:25:56 Jul 8
- ip sla schedule 9129 ip sla forever start-time 20:26:31 Jul 8
- ip sla schedule 9132 ip sla forever start-time 22:02:19 Jul 9 aggrnt 60
- ip sla schedule 9136 ip sla forever start-time 22:32:55 Jul 9
- ip sla schedule 9138 ip sla forever start-time 22:26:26 Jul 15 aggrnt 60
- ip sla schedule 9141 ip sla forever start-time 22:23:31 Jul 15
- ip sla schedule 9145 ip sla forever start-time 00:15:04 Jul 16 aggrnt 60
- ip sla schedule 9148 ip sla forever start-time 00:16:08 Jul 16
- ip sla schedule 9149 ip sla forever start-time 00:17:34 Jul 16 aggrnt 60
- ip sla schedule 9151 ip sla forever start-time 00:15:12 Jul 17 aggrnt 60
- ip sla schedule 9154 ip sla forever start-time 02:15:45 Jul 18
- ip sla schedule 9155 ip sla forever start-time 02:16:26 Jul 18 aggrnt 60

Diff View를 사용하여 두 구성 간의 구성 변경을 나란히 비교

색상 코드 변경 묘사를 사용하여 구성 파일 간의 변경 사항을 쉽게 식별

추가된 라인은 녹색으로, 삭제된 라인은 빨간색으로, 수정된 라인은 파란색으로 표시

Config Diff View

LHS

Select Device
192.168.50.140

Running StartUp Draft

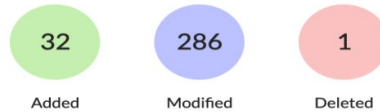
Select Config
Version 117

Changed By
Not Available

Backedup Time
Mar 15, 2019 11:01 AM

[View Annotation](#)

Startup Running Conflict Diff



Diff with Baseline



잘못된 변경 사항을 신속하게 찾아내고 즉시 복원

구성 비교

모든 유형의 구성, 두 장치(작동 및 비 작동)간에 비교를 수행 할 수 있습니다. 아래 이미지는 실행중인 구성과 시작 구성 사이의 모든 변경 사항을 비교 한 것입니다.

LHS - Running		RHS - Startup	
1088	ip sla schedule 522 life forever start-time 05:47:50 May 9 ageout 60	ip sla schedule 522 life forever start-time 05:47:51 May 9 ageout 60	
1098	ip sla schedule 524 life forever start-time 05:43:50 May 9	ip sla schedule 524 life forever start-time 05:43:51 May 9	
1290	ip sla schedule 556 life forever start-time 12:32:50 Jun 6 ageout 60	ip sla schedule 556 life forever start-time 12:32:51 Jun 6 ageout 60	
1571	logging trap notifications		
1735	line vty 0 4	line vty 0 1	
1740		line con 196 198	

역할 기반 액세스 제어 (ROLE-BASED ACCESS CONTROL: RBAC)

NCM은 데이터 오용을 방지하기 위해 세 가지 유형의 사용자에게 대한 권한을 제공합니다

- **Amin 관리자:** 모든 장치에 액세스하고 변경하는 권한 (1 명)
- **제한된 Admin 관리자(고급 사용자):** 권한이 부여된 특정 장치에 액세스하거나 변경하거나 다른 장치를 추가 또는 삭제할 수 있는 권한.
- **운영자(Operator):** 권한이 제한되어 있으며 고급 사용자 또는 관리자의 승인을 기다려 권한을 받아야 장치를 업로드하거나 변경할 수 있습니다.

구성 초안 편집 및 업로드: 관리자가 사용자의 변경을 승인하면, 업로드 되고 백업이 수행되며, Admin관리자는 직접 업로드 할 수 있습니다.

Edit as Draft

Content

```
voice-card 0
|
crypto pki token default removal timeout 0
|
crypto pki trustpoint TP-self-signed-2273236155
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2273236155
revocation-check none
|
crypto pki certificate chain TP-self-signed-2273236155
certificate self-signed 02
3082022B 30820194 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
46464643 4174452D 22222323 22222321 2E2E201E 170D3128 20262122 212E2121
```

Cancel Save Save and

Recent Changes [27]

Captured On	Host Name	IP Address	Version	Changed by	Config Type	Change Type	
Jun 13, 2018 21:01 PM	192.168.50.1 30	192.168.50.1 30	12	Not Available	Startup	Unauthorized	
Jun 13, 2018 21:01 PM	192.168.50.1 30	192.168.50.1 30	17	Not Available	Running	Unauthorized	
Jun 12, 2018 13:01 PM	192.168.50.1 30	192.168.50.1 30	11	Not Available	Startup	Unauthorized	

Role-Based Access Control (RBAC) 화면

Configure User Details

User Details
Provide the user role, credential and contact details.

Role: Operator

User Type: Local Authentication

User Name *

Password * [Configure password policy](#)

Email Id *

Scope
Configure permitted devices for a user to access.

Phone Number

Mobile Number

Re-type Password *

Time Zone (For NetFlow reports): Asia/Calcutta

Cancel Next

Upload Config

StartUp Running

You do not have upload permission. Click 'Upload' to place your request to the administrator.

While uploading Startup configuration, please make sure to upload full configuration content.

Cancel Upload

Approve Request

Selected Devices: 192.168.50.140

Configuration Used: show version

Execution Mode: Script Execution Mode

Trigger Configuration Backup: Disabled (before and after template execution)

Now Schedule

Approval / Rejection Comments

Cancel Reject Approve

RBAC를 사용하여 범위를 정의하여 네트워크 장치에 대한 사용자 액세스를 제한하고 제어

한 운영자(operator)가 구성을 변경하면 통지 수신

장치에 업로드하기 전에 변경 사항을 검토

네트워크 요구 사항에 따라 변경을 승인 / 거부

네트워크에 대한 완전한 가시성을 확보하고 무단 변경을 제한

실시간 변경 알림

Add Notification

Actions Associate

Notification Name: Backup

Description: Backup

Config Type: Startup or Running configuration is chan...

Change Type: Authorized or Unauthorized change

Email

Notify Email to: test@ncm.com
(Use , for multiple address)

Subject: Test

select variables: \$RULENAME

Message:

select variables: \$RULENAME

Email Format: Html

Append Configuration Difference in Message

Add Notification

Actions Associate

SNMP Trap

Hostname/ IP Address: 1.1.1.1

Destination Port: 162

Community: public

Syslog

Hostname/ IP Address:

Destination Port:

Ticket

Send Trouble Ticket to:

Ticket Subject: select variables: \$RULENAME

Ticket Message: select variables: \$RULENAME

네트워크 장치에서 실시간 변경 알림을 활성화

구성이 변경되면 알림을 받음

이메일, SNMP 트랩, syslog 메시지 형식으로 알림 수신.

방화벽과 같은 중요한 장치의 구성 변경 사항 복원

구성 템플릿(CONFIGLET)으로 자동화

Configlets 으로 자동화 달성

Configlets라고 하는 스크립트 템플릿을 실행하여 여러 장치에서 잘못된 구성을 수정하고 대량으로 변경합니다



- 반복 작업 자동화
- 대량 변경을 실행하여 시간 절약
- 오작동하는 장치를 한 번에 해결
- 수동 명령 실행 제거

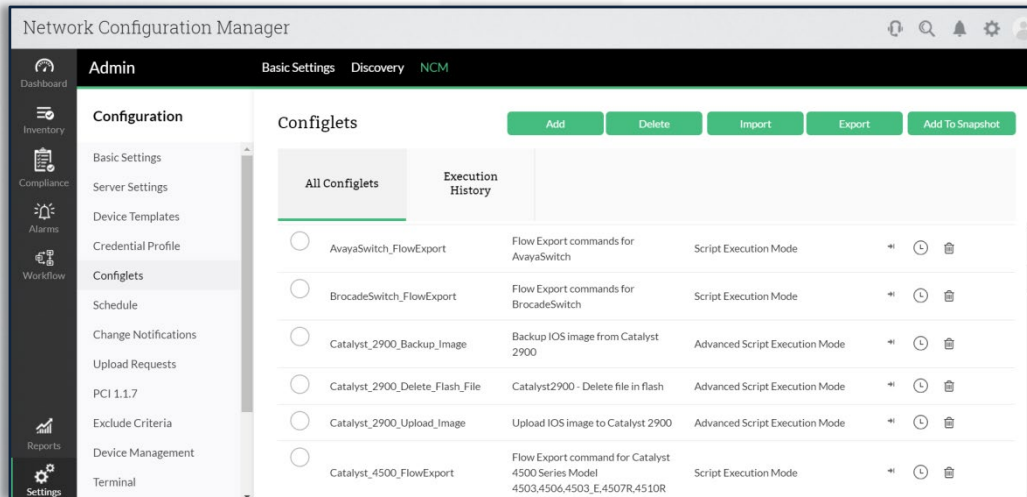
컨피그릿(Configlet) 과 그 사용

컨피그릿(Configlet)은 한 번에 여러 장치에서 실행할 수 있는 구성 용 스크립트 템플릿입니다.

장점:

- 컨피그릿(Configlet)은 템플릿으로 사용 가능하며 수동으로 추가할 수 있습니다.
 - 3가지 모드: 파일 전송, 스크립트 실행, 고급 스크립트 실행
- 한 번에 오작동하는 장치들을 동시에 수정하는 데 도움
- 한 번에 여러 장치에서 일련의 명령을 실행할 수 있습니다.

템플릿 :



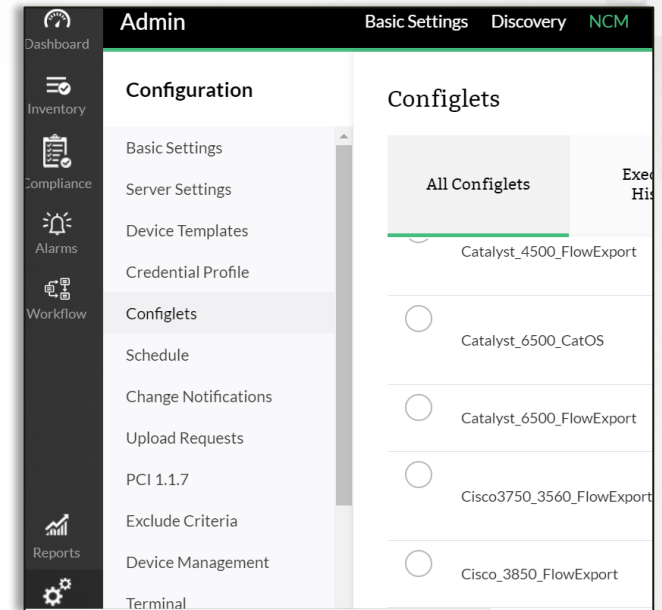
Network Configuration Manager

Admin Basic Settings Discovery NCM

Configuration

Configlets

All Configlets	Execution History
<input type="radio"/> AvayaSwitch_FlowExport	Flow Export commands for AvayaSwitch Script Execution Mode
<input type="radio"/> BrocadeSwitch_FlowExport	Flow Export commands for BrocadeSwitch Script Execution Mode
<input type="radio"/> Catalyst_2900_Backup_Image	Backup IOS image from Catalyst 2900 Advanced Script Execution Mode
<input type="radio"/> Catalyst_2900_Delete_Flash_File	Catalyst2900 - Delete file in flash Advanced Script Execution Mode
<input type="radio"/> Catalyst_2900_Upload_Image	Upload IOS image to Catalyst 2900 Advanced Script Execution Mode
<input type="radio"/> Catalyst_4500_FlowExport	Flow Export command for Catalyst 4500 Series Model 4503.4506.4503_E.4507R.4510R Script Execution Mode



Admin Basic Settings Discovery NCM

Configuration

Configlets

All Configlets	Execution History
<input type="radio"/> Catalyst_4500_FlowExport	
<input type="radio"/> Catalyst_6500_CatOS	
<input type="radio"/> Catalyst_6500_FlowExport	
<input type="radio"/> Cisco3750_3560_FlowExport	
<input type="radio"/> Cisco_3850_FlowExport	

Configlets 으로 명령 수행

Modify Configlet

Name
Alaxala_Enable_Change_detection

Execution Mode
Script Execution Mode

Description
Forward syslog messages to syslog server, applicable for Alaxala 5400 devices

Configlet Content
logger syslog %Syslog_IP% %Facility%.%Level% %Event_Level%

Configuration Backup
 Perform configuration backup before and after template execution

Cancel Save

Modify Configlet

Name
Upload startup config

Execution Mode
File Transfer Mode

Description
Upload startup config

Configlet Content
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<Configlets>
<Configlet>
<TEMPLATE_ID>301</TEMPLATE_ID>
<TEMPLATE_NAME>Startup_Config_Upload</TEMPLATE_NAME>
<TEMPLATE_TYPE>TFTP_FILE_TRANSFER_MODE</TEMPLATE_TYPE>
<OWNER_NAME>admin</OWNER_NAME>
<LAST_MODIFIED_TIME>2018-06-26 11:30:55.679</LAST_MODIFIED_TIME>
<DESCRIPTION>Standard configuration for all Cisco Devices</DESCRIPTION>
<TEMPLATE_CONTENTS>

!
! Last configuration change at 11:21:58 UTC Fri Jun 8 2018 by melab
version 15.3

Configuration Backup
 Perform configuration backup before and after template execution

Cancel Save

명령 실행 작업을 자동화하고
장애를 한 번에 해결

파일 전송 모드를 사용하여
구성을 여러 네트워크 장치에
대량 업로드

오류를 수정하고 스크립트
실행 모드를 사용하여 기본
구성 명령을 실행

고급 스크립트 실행 모드에서
사용자 확인이 필요한 복잡한
명령을 실행함

컨피그릿 수동 추가

파일 전송 모드

파일 전송 모드를 사용하면 사용자가 여러 장치로 동일한 구성을 한 번에 업로드 할 수 있다는 장점이 있습니다.

Add Configlet

Name
startup_config_upload

Execution Mode
File Transfer Mode

Description
upload config to selected devices

Configlet Content

```
ip sla reaction-configuration 386 react jitterSDAvg threshold-value 30 25 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 386 react packetLossSD threshold-value 1 1 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 386 react maxOflatencySD threshold-value 120 100 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 387 react rtt threshold-value 100 75 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 387 react mos threshold-value 500 350 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 387 react jitterSDAvg threshold-value 30 25 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 387 react packetLossSD threshold-value 1 1 threshold-type immediate action-type trapOnly
ip sla reaction-configuration 387 react maxOflatencySD threshold-value 120 100 threshold-type immediate action-type trapOnly
```

Configuration Backup
 Perform configuration backup before and after template execution

Cancel Save

Execute Configlet

Configlet Name
startup_config_upload

Execution Mode
File Transfer Mode

Selected Devices

Choose Devices or Device Group:
 Select Specific Device Select Device Group

Available Devices	Selected Devices
Search	Search
192.168.49.6	
192.168.50.130	
192.168.50.131	
192.168.50.140	
Tastine device	

Perform configuration backup before and after template execution

[Click here for more help](#)

Cancel Execute

스크립트 실행 모드

다음의 경우에 도움이 됨 :

- 기본 문제 해결 명령 실행
- 비밀번호, 배너 변경
- SNMP 활성화/비활성화

예: 특정 네트워크 장치를 선택하고 스크립트 실행 모드에서 실행하면 연계된 모든 장치의 암호가 변경됩니다.

	Cisco_Change_Password_Script	Changing Password for Cisco devices	Script Execution Mode			
--	------------------------------	-------------------------------------	-----------------------	---	---	---

Modify Configlet	
Name	Cisco_Change_Password_Script
Execution Mode	Script Execution Mode
Description	Changing Password for Cisco devices
Configlet Content	<pre>configure terminal enable password %PASSWORD% end</pre>

고급 스크립트 실행 모드

이 모드는 다음과 같은 경우에 사용됩니다.

1. 명령 실행 후 프롬프트 변경이 발생
2. 명령이 신속한 사용자 확인을 요구할 때
3. 명령 실행 후 응답이 지연될 때

예: 다음 예제에서, 명령은 특정 프롬프트 후에 실행되며 시간 초과도 설정됩니다.

Modify Configlet
Name
<input type="text" value="Cisco_Router_Backup_Image"/>
Execution Mode
<input type="text" value="Advanced Script Execution Mode"/>
Description
<input type="text" value="Backup IOS image from Cisco Routers"/>
Configlet Content
<pre><command prompt=']?'>copy flash:%IMAGE_FILENAME% tftp</command> <command prompt=']?'>%TFTP_SERVER_IP%</command> <command timeout='70'>%DESTINATION_FILE_NAME%</command></pre>

컨피그릿 실행

- 컨피그릿을 수정한 후 해당 장치에 컨피그릿을 적용하여 실행하고 "실행 기록"에서 실행 결과를 확인할 수 있습니다.
- 컨피그릿을 생성 한 후에는 쉽게 액세스 할 수 있도록 "스냅 샷"에 추가 할 수 있습니다.

Execute Configlet

Configlet Name
Cisco_Change_Password_Script

Execution Mode
Script Execution Mode

Template Variables
 Same value for all devices A different value for each device

PASSWORD
new password

Add To Snapshot

Alaxala_Enable_Change_detection

Vendor
3Com

Device Template Name
3Com 4200G Series Switch

Cancel Add To Snapshot

All Configlets	Execution History			
Configlet Name	Execution Status	Invoked On	Invoked By	
<input type="radio"/>	Cisco_Show_Version_Script	<input checked="" type="checkbox"/> COMPLETED	Jun 12, 2018 21:20 PM	admin

Configlets으로 펌웨어 업그레이드

라우터 및 스위치와 같은 네트워크 장치를 최신 OS 버전으로 업데이트

하드웨어 인벤토리를 사용하여 OS 버전을 확인하여 업그레이드할 장치를 식별

펌웨어를 업그레이드하여 기존 버전의 취약성 및 버그 수정.

스크립트 실행 모드를 사용하여 펌웨어를 대량으로 업그레이드

Add Configlet

Name
Firmware upgrade

Execution Mode
Script Execution Mode

Description
cisco firmware update

Configlet Content

```
<command prompt=']'>copy tftp: flash:</command>  
<command prompt=']'>%TFTP_SERVER_IP%</command>  
<command prompt=']'>%SOURCE_FILE_NAME%</command>  
<command prompt='confirm'>%DESTINATION_FILE_NAME%</command>  
<command timeout='120' suffix='$NO_ENTER'>y</command>
```

Configuration Backup
 Perform configuration backup before and after template execution

Execute Configlet

Configlet Name
AvayaSwitch_FlowExport

Execution Mode
Script Execution Mode

Selected Devices

Choose Devices or Device Group:
 Select Specific Device Select Device Group

Available Devices	Selected Devices
Search	Search
27.1.1.2	
27.1.1.3	
27.1.1.4	
27.1.1.5	
27.1.1.6	

Perform configuration backup before and after template execution

[Click here for more help](#)

Cancel Execute

Configlets 기타 장점

Network Configuration Manager

Dashboard Inventory Compliance Change Management Alarms Tools Settings Reports Support

Basic Settings Device Management Discovery User Management Configlets Schedule Global Settings PCI 1.1.7

Configlets Add Delete Import Export Add To Snapshot

All Configlets	Execution History					
Configlet Name	Description	Created By	Last Modified Time	Template Type		
<input type="radio"/> Alaxala_Enable_Change_detection	Forward syslog messages to syslog server, applicable for Alaxala 5400 devices	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> AlliedTelesis_87XX_Disable_Change_detection	Disable syslog for AlliedTelesis CenterCom 87XX	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> AlliedTelesis_87XX_Enable_Change_detection	Forward syslog messages to syslog server, applicable for AlliedTelesis CenterCom 87XX	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> AlliedTeleSwitch_sFlowExport	sFlowExport Commands for Allies TeleSwitch	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> AwayaSwitch_FlowExport	Flow Export commands for AwayaSwitch	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> BrocadeSwitch_FlowExport	Flow Export commands for BrocadeSwitch	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_2900_Backup_Image	Backup IOS image from Catalyst 2900	system	[NA]	Advanced Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_2900_Delete_Flash_File	Catalyst2900 - Delete file in flash	system	[NA]	Advanced Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_2900_Upload_Image	Upload IOS image to Catalyst 2900	system	[NA]	Advanced Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_4500_FlowExport	Flow Export command for Catalyst 4500 Series Model 4503,4506,4503_E,4507R,4510R	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_6500_CatOS	Flow Export command for Catalyst 6500 Model CatOS 6504_E,6513,6509,6506	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> Catalyst_6500_FlowExport	Flow Export command for Catalyst 6500 Model 650X and 1440_V55	system	[NA]	Script Execution Mode	*	🗑
<input type="radio"/> CDP	This command is to Displays detailed information about neighboring devices discovered using CDP	admin	Feb 07, 2019 22:53 PM	Script Execution Mode	*	🗑
<input type="radio"/> Cisco3750_3560_Flowexport	Flow export command for WS-C3560X-48PF-S and WS-C3560X-48T-S	system	[NA]	Script Execution Mode	*	🗑

ACL(액세스 제어 목록)을 사용하여 대역폭 병목 현상을 해결

SNMPV3을 구성하여 중요한 데이터를 보호

스위치에 VLAN을 구성하여 네트워크 유연성을 향상

Configlet을 사용하여 syslog 메시지를 전달

규정 준수 관리

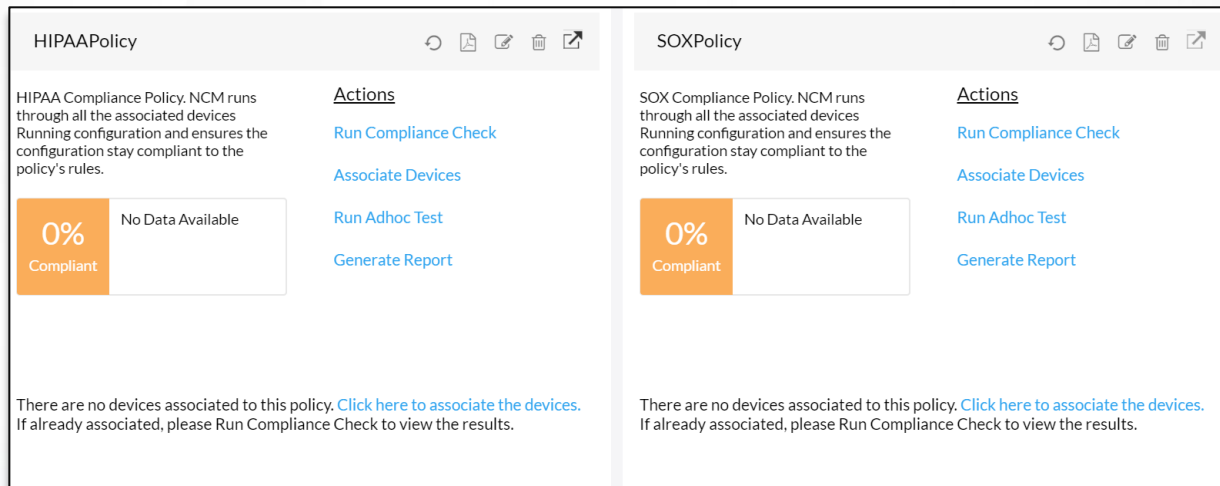
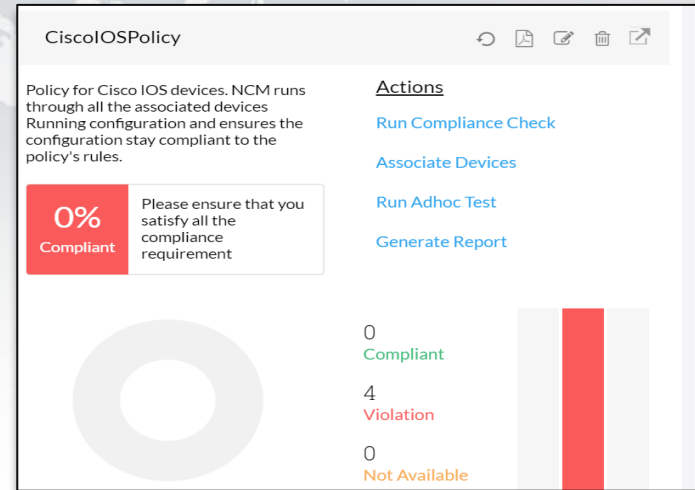
규정 준수가 필요한 이유는 무엇입니까?

장점:

- 취약점을 피하는 데 도움이 됩니다.
- 네트워크의 루프 홀 방지
- 법적 문제점 발생 방지

기본 규정 준수 정책 :

Cisco IOS 정책, HIPAA, SOX, PCI



기본 규정 준수 정책

HIPAAPolicy

HIPAA Compliance Policy. NCM runs through all the associated devices Running configuration and ensures the configuration stay compliant to the policy's rules.

0% Compliant Please ensure that you satisfy all the compliance requirement

Actions

- Run Compliance Check
- Associate Devices
- Run Adhoc Test
- Generate Report

0 Compliant
2 Violation
0 Not Available

CiscoIOSPolicy

Policy for Cisco IOS devices. NCM runs through all the associated devices Running configuration and ensures the configuration stay compliant to the policy's rules.

83% Compliant Please ensure that you satisfy all the compliance requirement

Actions

- Run Compliance Check
- Associate Devices
- Run Adhoc Test
- Generate Report

5 Compliant
1 Violation
0 Not Available

Cisco 장치 전용 규칙을 배포하여 Cisco 장치를 보호

PCI 규정 준수 보고서를 사용하여 PCI 규칙을 검토

PCI Report

Host Name	Review Status	Device Type	Model	Last Backup at
27.1.1.17	NOTASSIGNED	Cisco Router	2612	Mar 25, 2019 13:01 PM
27.1.1.12	NOTASSIGNED	Cisco Router	2612	Mar 25, 2019 14:34 PM
27.1.1.13	NOTASSIGNED	Cisco Router	2612	Mar 25, 2019 13:01 PM
27.1.1.42	NOTASSIGNED	Cisco Router	[NA]	Mar 25, 2019 13:01 PM

사용자 정의 정책

다음과 같은 방법으로 사용자 정의 정책을 추가 할 수 있습니다.

- 사용자 정의 규칙 만들기
- 사용자 정의 규칙을 그룹화하여 규칙 그룹 생성
- 정책을 만들기 위해 규칙 그룹 그룹화

사용자 정의 규칙은 3가지 기준에 따라 추가됩니다.

- 간단한 기준
- 고급 기준
- 고급 사용자 정의 기준

Add Compliance Rule

Criteria New Rule

Simple Criteria Advanced Criteria Advanced Custom Criteria

Configuration File

should contain all lines Any time(s).

Next

간단한 기준 - 예제

간단한 기준의 사용 :

- 한 구성에서 특정 행(line)을 포함하는지 확인
- 정확한 세트를 포함하거나 포함하지 않아야 함
- 해당 행이 나타나야 하는 횟수

Edit Compliance Rule

Criteria New Rule

Simple Criteria Advanced Criteria Advanced Custom Criteria

Configuration File

should not contain any line Any

```
snmp-server community public RO
snmp-server community public RW
```

Next

예:왼편 예에서 단어
“Public“ 이 선택되어 있습니다.

고급 기준 - 예제

복잡한 정규식을 사용하여 한 구성에서 특정 행(line)을 확인하는 데 사용합니다.

지원 정규식:

- AND/OR
- 패턴

Condition	Pattern	Time
should contain	snmp-server location \S+	Any
and	should contain	logging host \S+

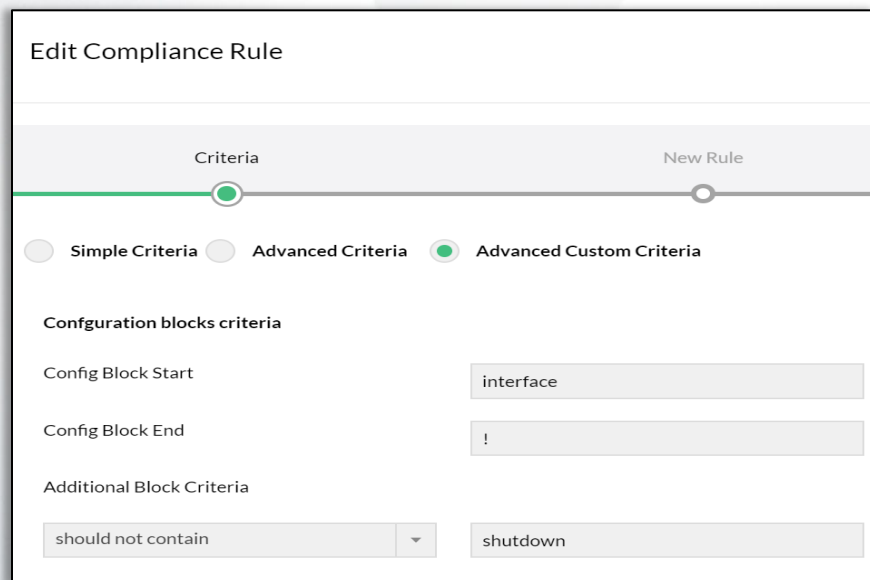
예:패턴 검색이
구현되었습니다.



고급 사용자 정의 기준 - 예제

이는 한 구성 파일의 특정 섹션에서 규정 준수 검사를 실행하려는 경우에 사용되며, 고급 기준의 기능을 함께 지원합니다.

1. 블록 기준(블록의 시작과 끝을 지정)
2. 추가 차단 기준



The screenshot shows the 'Edit Compliance Rule' interface. At the top, there are two tabs: 'Criteria' (selected) and 'New Rule'. Below the tabs, there are three radio buttons: 'Simple Criteria', 'Advanced Criteria', and 'Advanced Custom Criteria' (selected). Under the 'Configuration blocks criteria' section, there are two input fields: 'Config Block Start' with the value 'interface' and 'Config Block End' with the value '!'. Below this, there is an 'Additional Block Criteria' section with a dropdown menu set to 'should not contain' and a text input field containing 'shutdown'.

예제 :이 예제에서는

NCM이 “shut down“이 아닌

인터페이스에 대해서만 규정 준수
점검을 실행하도록 정의합니다.

교정 템플릿 (Remediation Template)

교정 템플릿은 규정 준수 검사 중에 특정 규칙의 위반이 발견될 때 사용됩니다. 위반이 있는 경우 문제를 수정하기 위해 교정 템플릿을 사용합니다.

예: snmp에서 "public"을 확인하는 동안, 구성에서 "public"이라는 단어가 발견되면 이 교정 템플릿을 사용하여 수정할 수 있습니다.

Edit Compliance Rule

Criteria New Rule

Simple Criteria Advanced Criteria Advanced Custom Criteria

Configuration File

should not contain any line Any

```
snmp-server community public RO
snmp-server community public RW
```

Edit Compliance Rule

Criteria New Rule

Violation Severity

Critical Major Warning

Remediation Description

Remove public community from config

Remediation Configlet

Cisco_Syslog_Configurations

규칙 그룹 및 정책 생성

사용자 정의 규칙은 규칙 그룹으로 그룹화되고 다시 정책으로 그룹화됩니다.
이제 이 정책은 선택된 네트워크 장치와 연계할 수 있습니다.

Edit Compliance Rule Group

Rule Group Name	Description
adv custom RG	

Available Rules	Selected Rules
Search	Search
SNMPLocationGiven	adv custom Rule
SNMPContactGiven	
DHCPServiceDisabled	
PADServiceDisabled	
DomainNameServiceDisabled	
NoIPHTTPTServer	
SyslogServerLoggingEnabled	
NoConsoleLogging	
SrPasswordEncryptionEnabled	
SrPasswordLengthEnabled	

Add Compliance Policy

Policy Details Associate

Policy Name	Description
rrttest	test

Configuration Type Running StartUp

Policy Violation Criteria

Any rule in this policy is violated

Only if a Critical or Major rule in this policy is violated

Available Rule Groups	Selected Rule Groups
Search	Search
adv custom RG	
CheckInterfaceRG	

Add Compliance Policy

Policy Details Associate

Available Device Groups Selected Device Groups

Search	Search
All Devices Group	
Backup Failure Group	
CiscoRouter Group	
CiscoSwitch Group	

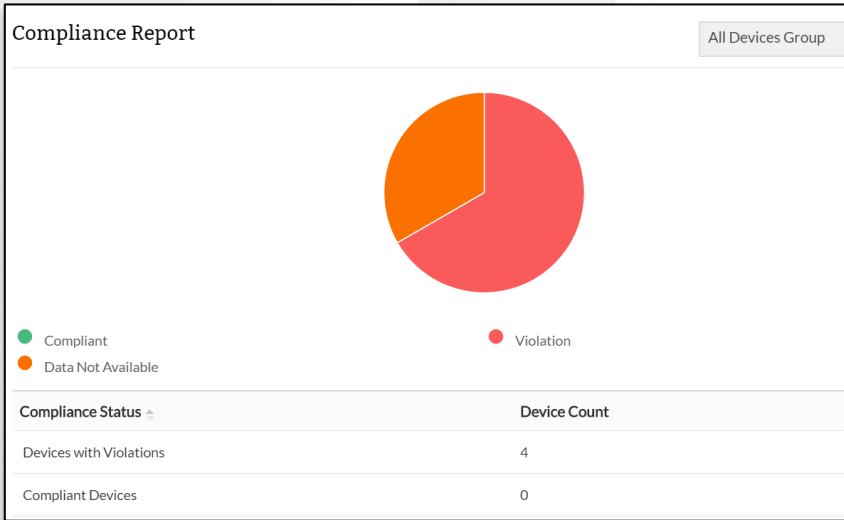
Available Devices Selected Devices

Search	Search
192.168.49.101	
192.168.49.6	
192.168.49.7	
192.168.50.130	

규정 준수 보고서

정책을 장치에 연계하면, 장치가 규정을 어떻게 준수하는지에 대한 보고서를 생성할 수 있습니다.

위반된 정책 및 규정 준수 장치를 확인할 수도 있습니다.



Violation Devices

Host Name	Critical	Major	Warning	Compliant	Last Check At
▶ 192.168.50.140	✖ 4	!! 5	! 3	👍 5	2018-06-19 11:01:04.668
▶ 192.168.49.7	✖ 4	!! 5	! 3	👍 5	2018-06-12 09:49:39.394
▶ 192.168.49.101	✖ 5	!! 6	! 3	👍 3	2018-06-12 09:49:39.332
▶ 192.168.50.131	✖ 5	!! 6	! 3	👍 3	2018-06-14 13:21:20.573

Page 1 of 1 | 50 | View 1 - 4

Compliant Devices

Host Name	Critical	Major	Warning	Compliant	Last Check At
-----------	----------	-------	---------	-----------	---------------

Network Configuration Manager

Dashboard Inventory **Firmware Vulnerability** Compliance Change Management Alarms Tools Settings Reports Support

Firmware Vulnerabilities

All 28 Critical 3 Important 12 Moderate 10 Low 3 Unrated 0

CVE ID	Base Score	Severity	No. of Affected Devices	Reference URL
▶ CVE-1999-0293	7.5	Important	55	https://www.cisa.gov/cybercert/2019-01-08-cybercert-19-001
▶ CVE-1999-0524	0	Low	55	https://www.cisa.gov/cybercert/2019-01-08-cybercert-19-001
▶ CVE-2000-0486	5	Moderate	55	https://www.cisa.gov/cybercert/2019-01-08-cybercert-19-001
▶ CVE-2004-0589	5	Moderate	55	https://www.cisa.gov/cybercert/2019-01-08-cybercert-19-001

Firmware 취약점 관리

Firmware 취약점 관리

이제 Network Configuration Manager를 사용하여 네트워크 장치에서 잠재적인 취약성을 식별하고 조치를 취할 수 있습니다.



- 네트워크의 모든 취약점 보기
- CVE(Common Vulnerabilities and Exposures) 세부 정보 및 심각도 보기
- 취약점 교정하기
- 고급 검색을 수행하고 검색과 관련된 모든 취약점 확인

네트워크의 모든 취약점 보기

Network Configuration Manager

Dashboard Inventory **Firmware Vulnerability** Compliance Change Management Alarms Tools Settings Reports Support

Firmware Vulnerabilities

All 20 Critical 3 Important 12 Moderate 10 Low 3 Unrated 0

CVE ID	Base Score	Severity	No. of Affected Devices	Reference URL
CVE-1999-0293	7.5	Important	55	https://vulntrc.org/cve-bin/cvname.cgi?name=CVE-1999-0293
CVE-1999-0524	0	Low	55	http://descriptions.securescout.com/tc/11011 http://blissjunior.net/Info-Center/index?page=content&id=JSA-10795 http://kb.warmware.com/selfservice/microsites/search.do?cmd=display&Context=1434 https://www.cvedb.org/?5 https://exchange.xforce.ibmcloud.com/vulnerabilities/306 https://exchange.xforce.ibmcloud.com/vulnerabilities/322 https://ic.mcafee.com/corporate/index?page=content&id=SB10053
CVE-2000-0486	5	Moderate	55	http://archives.mechaweb.com/archives/bugtraq/2000-05/0369.html http://archives.mechaweb.com/archives/bugtraq/2000-05/0370.html http://www.securityfocus.com/bid/1293 https://exchange.xforce.ibmcloud.com/vulnerabilities/4985
CVE-2004-0582	5	Moderate	55	http://www.cisco.com/warp/public/707/cisco-sa-20040616-bsp.shtml https://www.exploit-db.com/exploits/1784/

네트워크의 모든 취약성 목록과 이러한 취약점의 영향을 받는 장치의 수 표시

특정 CVE ID와 관련된 취약점에 대한 세부 정보 표시

즉시 최적의 교정 방법을 수행.

Network Configuration Manager

Dashboard Inventory **Firmware Vulnerability** Compliance Change Management Alarms Tools Settings Reports Support

CVE-1999-0293 7.5 Important Published Jan 01, 1998 05:00:00 Last Updated Sep 09, 2008 12:34:00

Summary
AAA authentication on Cisco systems allows attackers to execute commands without authorization.

Reference URL
<https://vulntrc.org/cve-bin/cvname.cgi?name=CVE-1999-0293>

Comment [NA]

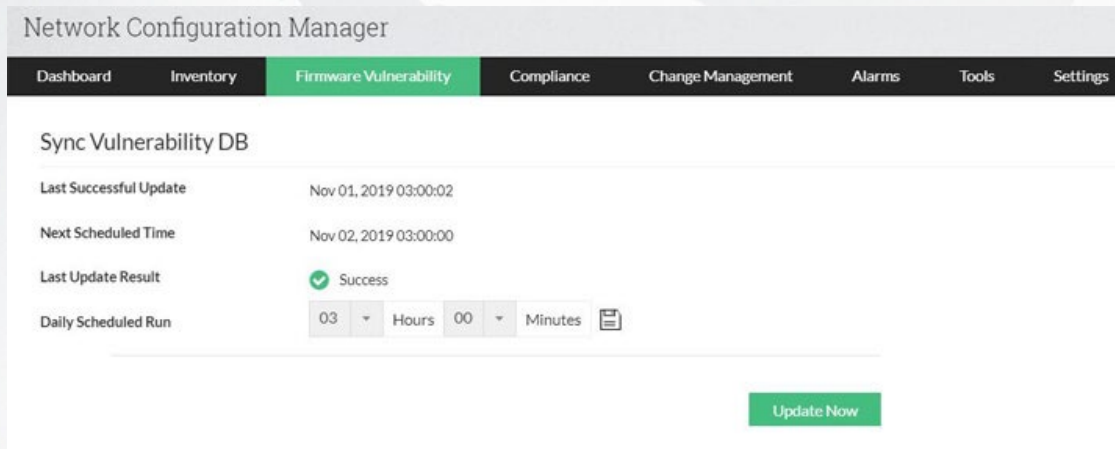
Reported

Host Name	State
27.1.1.42	Reported
test12	Confirmed
Cisco 50.140	Reported
192.168.50.131	Reported
27.1.1.30	Confirmed


"기본 점수"를 기준으로 취약점의 심각도를 분류

진행률을 기준으로 취약점 상태를 표시

Firmware 취약점 DB 동기화



The screenshot shows the 'Network Configuration Manager' interface with the 'Firmware Vulnerability' tab selected. The 'Sync Vulnerability DB' section displays the following information:

Last Successful Update	Nov 01, 2019 03:00:02
Next Scheduled Time	Nov 02, 2019 03:00:00
Last Update Result	✔ Success
Daily Scheduled Run	03 Hours 00 Minutes 

An 'Update Now' button is visible at the bottom right of the sync section.

NIST의 취약점 데이터는 Network Configuration Manager의 DB와 동기화 가능

일 단위로 데이터를 동기화하기 위해 예약 시간을 설정 가능.

스케줄 시간이 설정되지 않은 경우 기본적으로 매일 밤 새벽 2시에 동기화가 수행됨. 즉시 DB 동기화를 원할 경우 "Update Now" 옵션 사용 가능..

고급 CVE 검색

Network Configuration Manager

License will expire in 22 days | Get Quote | Purchase | Request Demo

Dashboard | Inventory | **Firmware Vulnerability** | Compliance | Change Management | Alarms | Tools | Settings | Reports | Support

Q cisco integrated services router

Processing 334 of 334 matches from 225475 total cve

Search Stop

CVE ID	Affected Releases
CVE-2017-12223	cisco lr800 integrated services router firmware
CVE-2013-1241	cisco c881w integrated services router
CVE-2014-3347	cisco 1861 integrated service router
CVE-2017-6721	cisco wide area application services 6.3(1)
CVE-2018-0327	cisco identity services engine software 2.1(0.905)
CVE-2018-0329	cisco wide area application services 6.4(1) , cisco wide area application services 6.2(3)
CVE-2013-3469	cisco mobility services engine
CVE-2012-1348	cisco wide area application services 5.1
CVE-2014-3285	cisco wide area application services 5.1 , cisco wide area application services 5.2
CVE-2018-0339	cisco identity services engine software 2.4(0.126) , cisco identity services engine software 2.3(0.298)
CVE-2012-5723	cisco air 1002 fixed router , cisco air 1023 router
CVE-2014-2183	cisco air 1009 fixed router , cisco air 1033 router

Page 1 of 14 | View 1 - 25 of 33

모든 취약점을 전반적으로 검색

제조사 이름, CVE ID, 장치 OS 번호, 버전 또는 모델을 사용하여 검색

특정 CVE ID에 해당하는 취약성에 대한 모든 세부 정보를 볼 수 있음.

Network Configuration Manager

Dashboard	Inventory	Compliance	Change Management	Alarms	Tools	Settings	Reports
<input type="radio"/> Devices (57)	<input checked="" type="radio"/> Groups (11)	<input type="radio"/> Configs (110)	<input type="radio"/> Changes (5155)	<input type="radio"/> Drafts (34)			
Device Group Name	Startup-Running Conflict Status						
<input type="radio"/> All Devices Group							
<input type="radio"/> Backup Failure Group							
<input type="radio"/> Cisco Group							
<input type="radio"/> CiscoRouter Group							
<input type="radio"/> CiscoSwitch Group	No device available						
<input type="radio"/> HP group	No device available						
<input type="radio"/> sai							
<input type="radio"/> Test	No device available						
<input type="radio"/> Test-Cisco							
<input type="radio"/> Testdpu							
<input type="radio"/> testsuccess							

재난 관리

Device Group Name: All Devices Group
 Startup-Running Conflict Status:

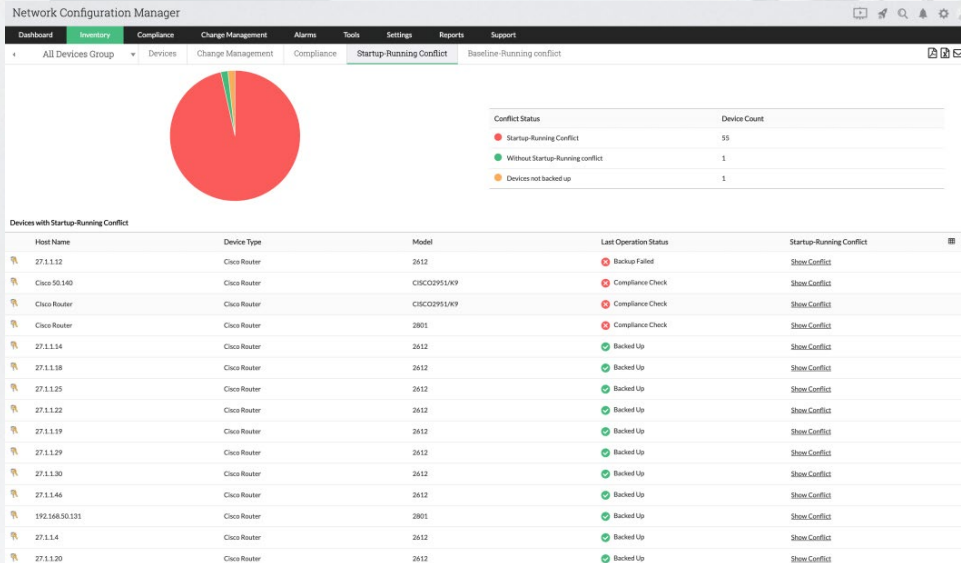
네트워크 재난 관리

네트워크 장애는 종종 영업 기회 손실, 고객 충성도 저하 및 직원 사기 저하로 이어집니다.
다음은 통해 현명하게 관리할 수 있습니다:



- 가장 안정적인 구성 복원
- Startup-Running 구성 동기화
- 로컬 저장소에 전체 데이터베이스 내보내기 및 저장
- 변경 알림 수신 및 중요 장치의 구성 복원

Startup-Running 구성 동기화

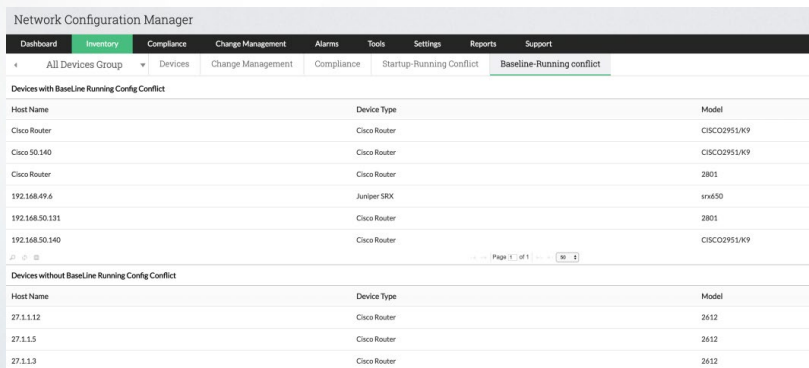


Startup-Running 실행 구성을 동기화하여 구성 변경/데이터 손실을 방지

startup-running 구성 간의 변경 내용 보기

Startup-Running 충돌에 대한 업데이트를 받고, 클릭한 번으로 동기화.

Startup-Running 충돌에 대한 상세 보고서 생성



Baseline 구성

Upload Config

Host Name: 27.1.1.17 Label: BASELINE

configuration upload to this device is not supported.

Host Name	Config Type	Version
27.1.1.17	Running	Version 1
27.1.1.17	Startup	Version 1

Page 1 of 1 50 View 1 - 2 of 2

Cancel

NCM Label Config

Selected Device(s): 27.1.1.17

Select Label to associate: BASELINE

Description: This label marks the stable configuration of a device

Cancel Save

한 변경이 발생하면, 구성 버전 수를 증가하여 저장합니다.

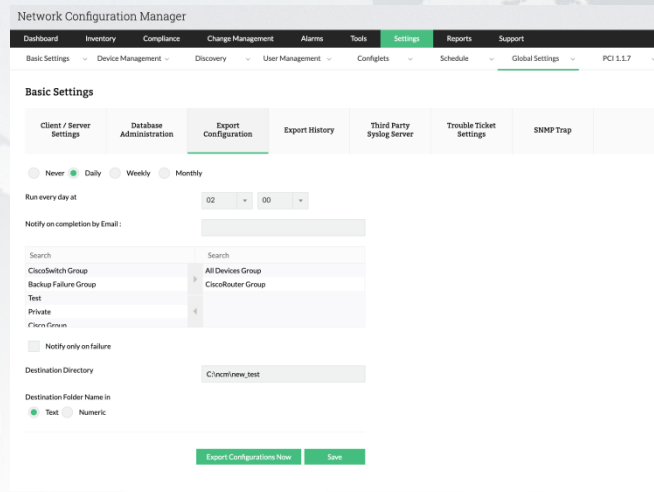
예: version 1.1 => version 1.2

레이블을 사용하여 구성 버전을 분류하여 쉽게 식별합니다.

가장 안정적인 구성 버전을 선택하고 Baseline 구성의 레이블로 지정합니다.

문제 발생 시, 즉시 Baseline 버전을 업로드하여 복원합니다.

구성 내보내기



구성을 내보내, 외부에서
보관하여, 심각한 네트워크
중단을 극복

전체 구성 데이터베이스의
복사본을 로컬 저장소에 저장

네트워크 중단 시 모든 구성을
장치에 업로드하고 네트워크
다운타임을 방지

회사 방침에 따라 구성
내보내기를 예약

Started On	Finished On	Execution Type	Status
Mar 25, 2019 02:00 AM	Mar 25, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 24, 2019 02:00 AM	Mar 24, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 23, 2019 02:00 AM	Mar 23, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 22, 2019 02:00 AM	Mar 22, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 21, 2019 02:00 AM	Mar 21, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 20, 2019 02:00 AM	Mar 20, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 19, 2019 02:00 AM	Mar 19, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 18, 2019 18:53 PM	Mar 18, 2019 18:53 PM	On Demand	SUCCESS
Mar 18, 2019 02:00 AM	Mar 18, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 17, 2019 02:00 AM	Mar 17, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 16, 2019 02:00 AM	Mar 16, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 15, 2019 02:00 AM	Mar 15, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 14, 2019 02:00 AM	Mar 14, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 13, 2019 02:00 AM	Mar 13, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 12, 2019 02:00 AM	Mar 12, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 11, 2019 02:00 AM	Mar 11, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 10, 2019 02:00 AM	Mar 10, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 09, 2019 02:00 AM	Mar 09, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 08, 2019 02:00 AM	Mar 08, 2019 02:00 AM	SCHEDULED	SUCCESS
Mar 07, 2019 02:00 AM	Mar 07, 2019 02:00 AM	SCHEDULED	SUCCESS

보고서

Network Configuration Manager

Dashboard Inventory Compliance Change Management Alarms Tools Settings Reports **Support**

Network Reports

Hardware Inventory Report

Hardware details listing the components and their status of the devices

Firmware Inventory

Firmware details listing the OS version and associated information of the devices

Device Inventory

Device details listing the model number, series and type of the devices

Network Health Status

Overview of the conflicts and compliance status of the device configurations

Device Management Status

Overview of device management setup status like credentials, real-time change detection etc.

Device Audit

Details on 'who', 'when' and 'what' of all the operations performed on the devices

Configuration Reports

Startup-Running Conflict

Details on the devices whose startup and running configurations differ

Configuration Changes

Details on the devices that have undergone change in configuration

Configuration Change Trend

Details on the number and type of configuration changes, during a specific time period

Configuration Analysis Report

Complete details about device configuration settings

Security Audit Report

Details on the findings of security audit together with the impact and recommendations

User Reports

User Access

Details on user access permission for all the devices

Configuration Upload Request

Overview of the status of configuration upload requests raised by the users

User Audit

Details of the operations performed by various users using the application

Other Reports

EOL/EOS Report

End-of-life and end-of-sale details about the devices

Compliance Report

Details on the violations and compliance of associated policies of the devices

PCI Report

Reports

보고서를 이용하여 구성 분석

네트워크 관리에서 주요 실책은 근본 원인을 분석하는 대신 임시 수정 사항을 구현하는 것입니다.
구성을 분석하고 광범위한 보고서를 통해 네트워크 문제의 원인을 제거하십시오!



구성 변경 세부 정보를 보기

하드웨어 정보에 대한 세부 정보를 가져오기

사용자 활동에 대한 보고서를 생성.

규정 준수 상태를 확인

서비스 종료를 앞둔 장치 목록 보기

네트워크 보고서

Network Configuration Manager

Dashboard Inventory Compliance Change Management Alarms Tools Settings **Reports** Support

Network Reports Configuration Reports EOL/EOS Report Compliance Report User Reports PCI Report Custom Report

Hardware Inventory Report

Device Group: All Devices Group Showing: 1 to 10 of 57 Page 1 View per page 10

192.168.49.101

IP Address	: 192.168.49.101	Series & Model	: 2801 & 2801	MAC Address	: [NA]
Device Type	: CiscoRouter	OS Type & OS Version	: IOS & 15.1(3)T1	Serial Number	: FHK1112F402
Image File	: c2801-adventerprisek9-mz.151-3T1.bin				

General Properties

IP Address	: 192.168.49.101	Series & Model	: 2801 & 2801
Device Type	: CiscoRouter	OS Type & OS Version	: IOS & 15.1(3)T1
System Location	: Not Available	End Of Sale Date	: Not Available
System Description	: Not Available	End of Support Date	: Not Available

Chassis Details

Serial No	: FHK1112F402	MAC Address	: [NA]
CPU	: Not Available	Flash Size	: 62720K
CPU Revision	: revision 6.0	Configuration Register	: 0x2102
DRAM Size	: 241664K/20480K	NVRAM Size	: 191K

Inventory

Name	Description	Product Identifier	Version Identifier	Serial Number
chassis	2801 chassis	[NA]	[NA]	[NA]
motherboard	C2801 Motherboard with 2 Fast Ethernet	CISCO2801	V03	FOC11095Y2D
PVDM0	PVDM0 DSP SIMM with two DSPs	PVDM0-32	V01	FOC110755K1
PVDM1	PVDM0 DSP SIMM with one DSP with half channel capacity	PVDM0-8	V01	FOC11080T57

192.168.49.7

IP Address	: 192.168.49.7	Series & Model	: C2951 & CISCO2951/K9	MAC Address	: [NA]
------------	----------------	----------------	------------------------	-------------	--------

하드웨어 세부 정보 및 장치 상태 보기.

모든 구성 작업에 대한 장치 상태 확인.

각 장치에 대한 자격 증명(패스워드)을 확인

장치 정보와 함께 펌웨어 버전에 대한 보고서

- Hardware Inventory Report**
Hardware details listing the components and their status of the devices
- Firmware Inventory**
Firmware details listing the OS version and associated information of the devices
- Device Inventory**
Device details listing the model number, series and type of the devices
- Network Health Status**
Overview of the conflicts and compliance status of the device configurations
- Device Management Status**
Overview of device management setup status like credentials, real-time change detection etc
- Device Audit**
Details on 'who', 'when' and 'what' of all the operations performed on the devices

Network Configuration Manager

Dashboard Inventory Compliance Change Management Alarms Tools Settings **Reports** Support

Network Reports Configuration Reports EOL/EOS Report Compliance Report User Reports PCI Report Custom Report

Firmware Inventory

Device Group: All Devices Group

Device Type	OsType	OsVersion	DeviceCount
+ Cisco Router	IOS	11.3(3)	50
+ Cisco Router	IOS	15.1(3)T1	2
+ Cisco Router	IOS	15.3(2)T	3

HostName

IP Address	Series	Model
Cisco 50.140	C2951	CISCO2951/K9
Cisco Router	C2951	CISCO2951/K9
192.168.50.140	C2951	CISCO2951/K9

IP Switch

IP Address	Series	Model
[NA]	[NA]	[NA]

Juniper SRX

IP Address	Series	Model
JunOS	9.6R2.11	

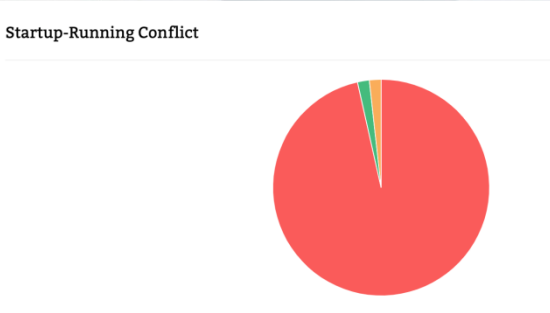
구성 보고서

모든 구성 변경 사항에 대한 세부 정보 보기

특정 기간 동안의 변경 사항 분석.

장치 구성 설정에 대한 세부 정보 찾기

Startup-Running 구성 간의 충돌 보고서 보기



Conflict Status	Device Count
Startup-Running Conflict	55
Without Startup-Running conflict	1
Devices not backed up	1

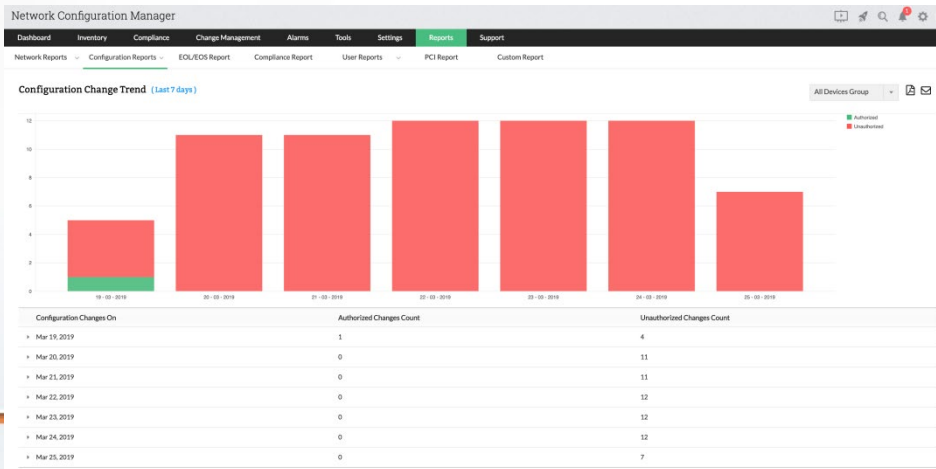
Network Configuration Manager

Configuration Changes (Last 7 days)

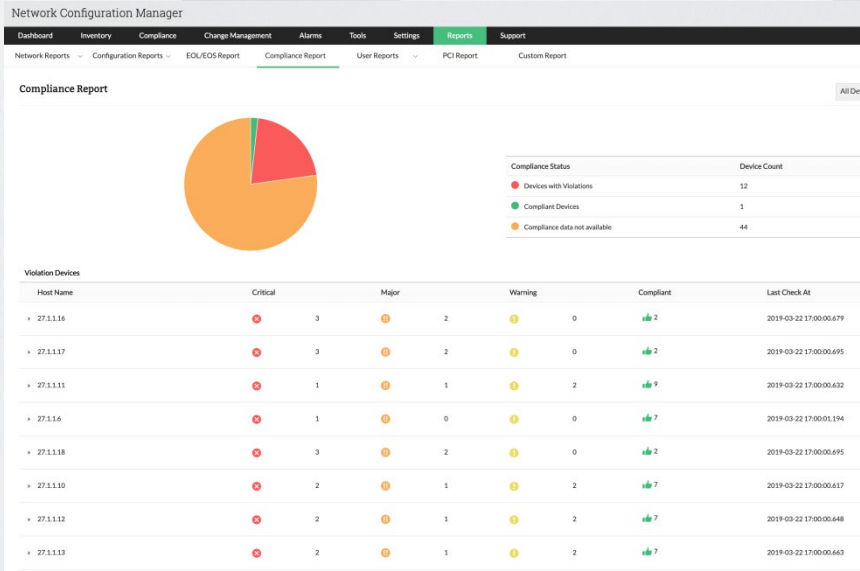
Change Type	Device Count
Devices with Configuration Changes	2
Devices without Configuration Changes	55

Host Name	Device Type	Model	Change Count
192.168.50.131	Cisco Router	2801	Authorized: 1 Unauthorized: 0
192.168.50.140	Cisco Router	CISCO2951-K9	Authorized: 21 Unauthorized: 4312

Host Name	Device Type	Model	Last Operation Status
Cisco-50.140	Cisco-Router	CISCO2951-K9	ComplianceCheck
27.1.1.12	Cisco-Router	CISCO2951-K9	ComplianceCheck
192.168.49.4	HP-Switch	1941	Backup
Cisco-Router	Cisco-Router	2801	ComplianceCheck
27.1.1.14	Cisco-Router	2612	Backup
27.1.1.18	Cisco-Router	2612	Backup
27.1.1.23	Cisco-Router	2612	Backup



다른 중요 보고서



Custom Report

Report Name	Report Description	Report Type
Abcd		compliance_report
Cisco Router Chassis Details	This report contains the Chassis Details of all Cisco Routers	network_report
Cisco Router General Properties	This report contains the general properties of all Cisco Routers	network_report
Cisco Switch Chassis Details	This report contains the Chassis Details of all Cisco Switch	network_report
Cisco Switch General Properties	This report contains the general properties of all Cisco Switch	network_report
Cisco OSPolicy report for CiscoRouters	This report contains the Cisco OSPolicy details of all Cisco Routers	compliance_report
Cisco OSPolicy report for CiscoSwitch	This report contains the Cisco OSPolicy details of all Cisco Switch	compliance_report

Add Custom Report

Report Name

Report Description

Report Type
Hardware Inventory Report

Select Device Template
3Com 5500 Series Switch

Choose Devices or Device Group:
 Select Specific Device
 Select Device Group

Available Devices	Selected Devices
Search	Search

Columns	Selected Columns
Search	Search
MACADDRESS	
IMAGEFILENAME	
Hardware Version	
SERIALNUMBER	
IPADDRESS	

Cancel Save

사용자 감사 보고서를 사용하여 사용자 액세스 권한에 대한 세부 정보

EOL/EOS 보고서를 통해 서비스 종료를 앞둔 기기 파악

규칙 위반 및 규정 준수 상태 준수 보고서 보기

회사 요구 사항에 따라 사용자 지정 보고서 생성.

NCM 보고서

NCM은 구성/규정 시행에 대한 많은 보고서를 생성합니다.

NCM Reports
Hardware Inventory Report
Firmware Inventory
Device Inventory
Network Health Status
Device Management Status
Device Audit
Startup-Running Conflict
Configuration Changes
Configuration Change Trend
EOL/EOS Report
Compliance Report
Configuration Analysis Report
Security Audit Report
PCI Report
User Access
Configuration Upload Request
User Audit
Custom Report

1. 구성 변경 보고서
2. 구성 변경 경향
3. EOL/EOS 보고서
4. 규정 준수 보고서
5. 구성 분석 보고서
6. 보안 감사 보고서

상세 보고서













NCM은 상세 보고서를 PDF 형식으로 생성합니다.

예: 장치 관리 상태 보고서

Report Details

For Device Group : All Devices Group

Associated Devices 192.168.50.131, 192.168.50.130, 192.168.49.7, 192.168.49.6, 192.168.50.140, 192.168.49.101

Host Name	Last Backup at	Credentials	Protocol Used	Real-time Change Detection
192.168.49.101	May 10, 2018 03:01 PM		TELNET	
192.168.50.131	Jun 19, 2018 01:02 PM		TELNET - TFTP	
192.168.50.130	Jun 19, 2018 01:01 PM		SSH	
192.168.49.7	May 10, 2018 07:01 AM		SSH	
192.168.49.6	Jun 19, 2018 01:01 PM		SSH	
192.168.50.140	Jun 19, 2018 01:01 PM		SSH	

인벤토리 정보

Network Configuration Manager

Dashboard | **Inventory** | Compliance | Change Management | Alarms | Tools | Settings | Reports | Support

Devices (57) | Groups (13) | Configs (103) | Changes (135) | Drafts (34)

contains public

Processing 100% of 5265 versions. 136 matches found.

IP Address	File Type	Version No	Captured On	Changed by
192.168.50.140	Running	4230	Mar 25, 2019 13:01 PM	nfa
192.168.50.140	Running	4229	Mar 25, 2019 11:01 AM	ajw
192.168.50.140	Running	4228	Mar 25, 2019 09:01 AM	ajw
192.168.50.140	Running	4227	Mar 25, 2019 07:01 AM	ajw
192.168.50.140	Running	4226	Mar 25, 2019 05:01 AM	ajw
192.168.50.140	Running	4225	Mar 25, 2019 03:01 AM	ajw
192.168.50.140	Running	4224	Mar 25, 2019 01:01 AM	ajw
192.168.50.140	Running	4223	Mar 24, 2019 23:01 PM	ajw
192.168.50.140	Running	4222	Mar 24, 2019 21:01 PM	ajw
192.168.50.140	Running	4221	Mar 24, 2019 19:01 PM	ajw
192.168.50.140	Running	4220	Mar 24, 2019 17:01 PM	ajw
192.168.50.140	Running	4219	Mar 24, 2019 15:01 PM	ajw
192.168.50.140	Running	4218	Mar 24, 2019 13:01 PM	ajw
192.168.50.140	Running	4217	Mar 24, 2019 11:01 AM	ajw
192.168.50.140	Running	4216	Mar 24, 2019 09:01 AM	ajw
192.168.50.140	Running	4215	Mar 24, 2019 07:01 AM	ajw
192.168.50.140	Running	4214	Mar 24, 2019 05:01 AM	ajw
192.168.50.140	Running	4213	Mar 24, 2019 03:01 AM	ajw

모든 하드웨어/소프트웨어 자산 세부 정보에 대한 자동 업데이트

각 네트워크 구성 작업의 상태 추적.

단일 콘솔에서 네트워크에서 탐색된 모든 장치 관리.

파악하려는 상태에 따라 필터를 적용하여 보기

인벤토리의 고급 검색 옵션을 사용하여 한 구성에서 원하는 문자열을 검색

Select columns

- Host Name
- IP Address
- Device Type
- Series
- Model
- OS Type
- OS Version
- Last Operation Status
- Config Conflict

Cancel Ok

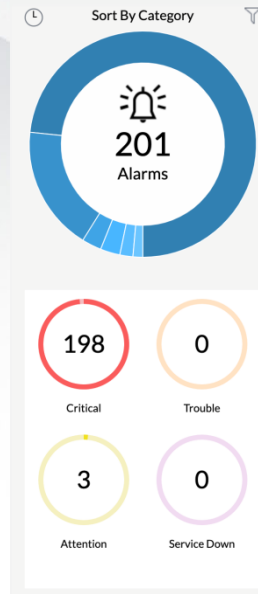
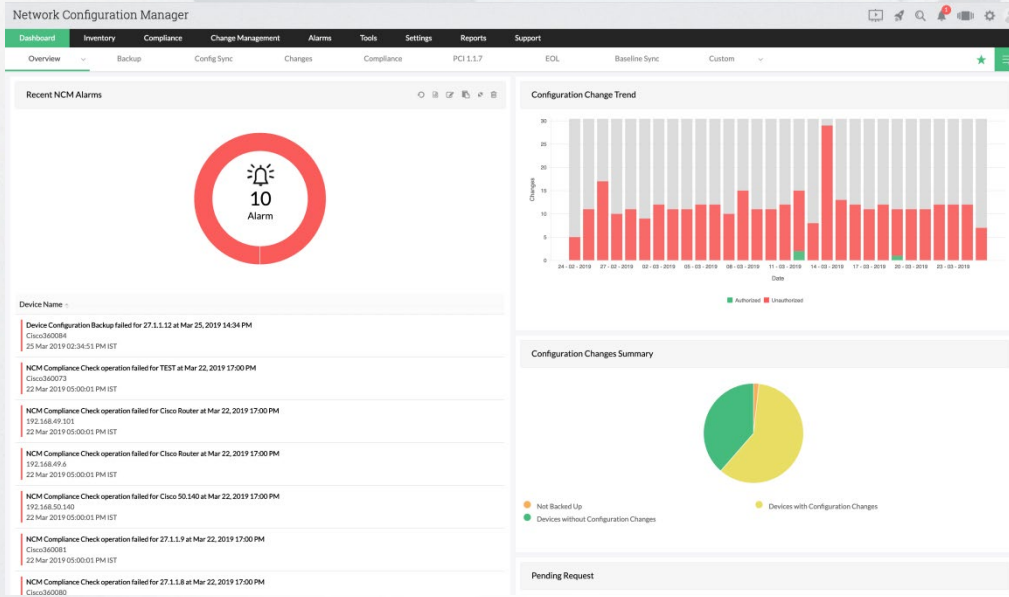
Search by Hardware Details

Device Type
3Com 5500 Series Switch

Boot Version

Cancel Search

대시보드, 그룹, 예약 & 경보

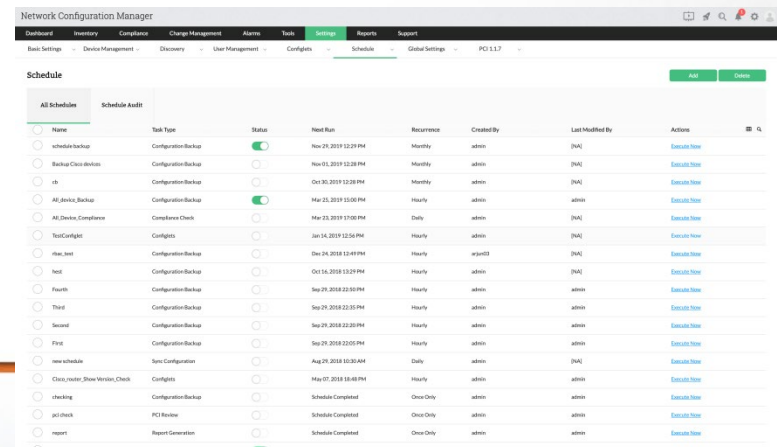
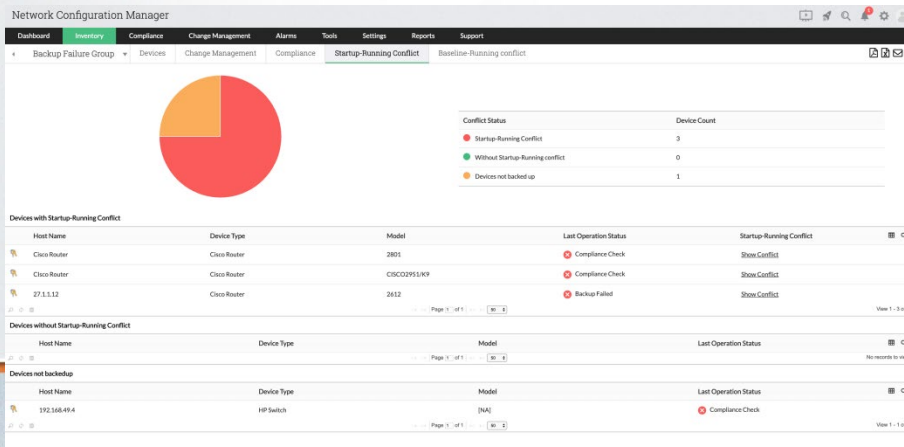


기능 별로 사용자 지정 대시보드

자동 동적 그룹을 사용하여 수동 분류 오류 감소

중요한 구성 작업을 예약

결함 있는 작동 중에 경보가 자동으로 트리거됨



NCM에서 일정 예약

- NCM의 모든 작업에 대해 예약을 수행 할 수 있습니다.
- 예약할 장치가 추가되고, 예약 시간이 지정됩니다.
- 해당 일정에 대한 통지가 설정됩니다.

Schedule Add Delete

All Schedules Schedule Audit

<input type="radio"/>	Name	Task Type	Status	Next Run	Recurrence	Created By	Last Modified By
<input type="radio"/>	All_device_Backup	Configuration Backup	<input checked="" type="checkbox"/>	Jun 19, 2018 13:00 PM	Hourly	admin	admin
<input type="radio"/>	Cisco_router_Show Version_Check	Configlets	<input type="checkbox"/>	May 07, 2018 18:48 PM	Hourly	admin	admin
<input type="radio"/>	All_Device_Compilance	Compliance Check	<input type="checkbox"/>	Mar 29, 2018 17:00 PM	Daily	admin	[NA]
<input type="radio"/>	checking	Configuration Backup	<input type="checkbox"/>	Schedule Completed	Once Only	admin	[NA]

Choose Devices or Device Group:

Select Specific Device Select Device Group

Available Devices	Selected Devices
<input type="text" value="Search"/>	<input type="text" value="Search"/>
192.168.49.6	
192.168.49.7	
192.168.49.101	

Add Schedule

Schedule name

Schedule Type

Notify if there is a failure in backing up a device

Exclude configuration difference from notification.

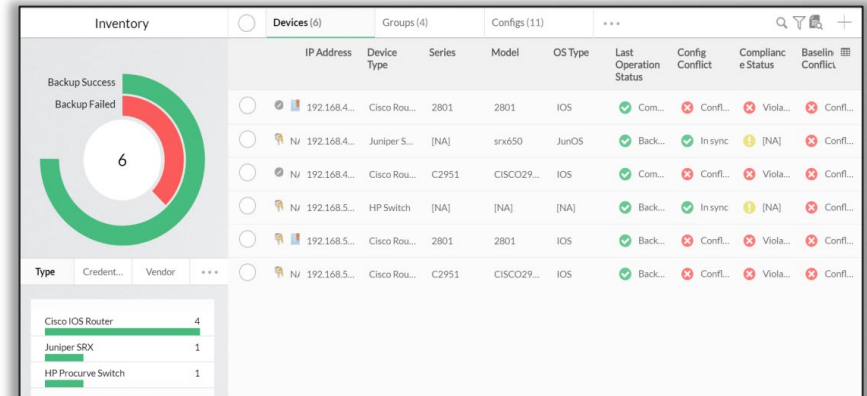
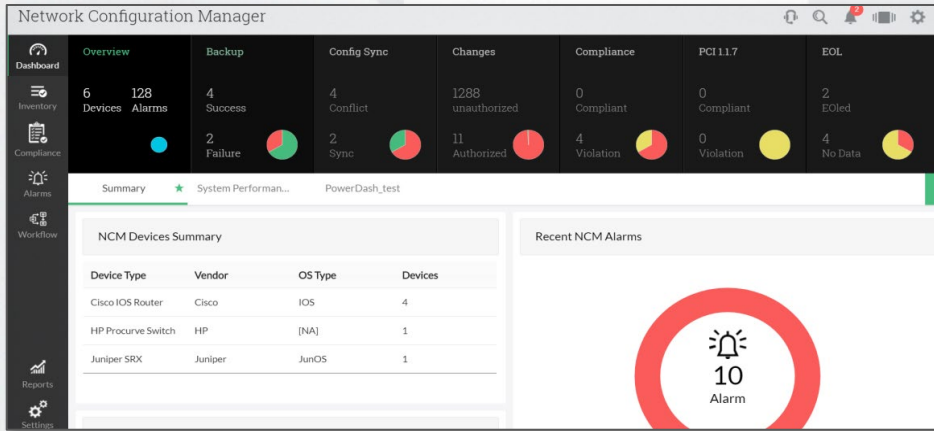
Notify if there is a change in configuration

Choose Devices or Device Group:

Select Specific Device Select Device Group

대시 보드 및 인벤토리

NCM의 대시 보드에는 네트워크 상태가 표시되며, 인벤토리는 계층적 순서의 구성 파일로 구성됩니다.



NCM에서 설정

설정은 기본, 탐색 및 NCM 설정으로 구성되며, 대부분의 작업이 이 작업을 통해 수행됩니다.

The screenshot displays the Network Configuration Manager (NCM) web interface. The top navigation bar includes 'Admin', 'Basic Settings', 'Discovery', and 'NCM', with 'Basic Settings' highlighted by a red box. The left sidebar lists various menu items under 'Configuration', 'Compliance', 'Alarms', 'Workflow', and 'Reports'. The main content area is titled 'Basic Settings' and features a horizontal menu with options: 'Client / Server Settings', 'Database Administration', 'Export Configuration', 'Export History', 'Third Party Syslog Server', and a 'more' dropdown. Below this, the 'General' section contains a 'Maximum diff limit (lines)' input field set to '5000'. A red 'Note' states: 'If number of line changes between two different configurations exceeds Maximum diff limit, you cannot view the changes in GUI.' At the bottom, there are two checkboxes: 'Enable auto SSH/Telnet' (checked) and 'Disable Resolve DNS' (unchecked).



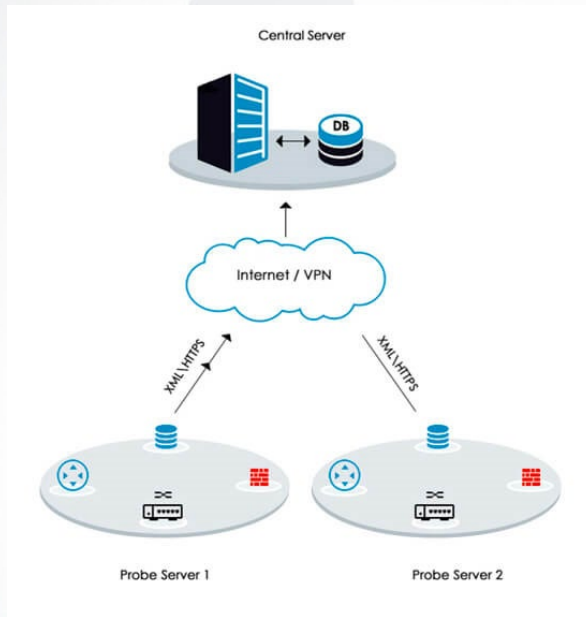
알람(경보)

작업 활동이 위반되면, NCM에서 경보를 보냅니다.

The screenshot displays the Network Configuration Manager (NCM) interface. The main heading is "Network Configuration Manager". The left sidebar contains navigation options: Dashboard, Inventory, Compliance, Alarms (selected), Workflow, and Reports. The top navigation bar includes a search icon, a notification bell with a red "2" badge, and a settings gear icon. The "Alarms" section is active, showing "Active Alarms (130)". A large circular gauge displays "130 Alarms". Below the gauge, two smaller gauges show "100 Critical" and "0 Trouble". The main content area lists 10 active alarms, each with a radio button, a description, device ID, type, status, and severity, and a timestamp of "92 days ago".

Radio	Alarm Description	Device ID	Type	Status	Severity	Timestamp	Actions
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.61 at Mar ...	Cisco360083	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.56 at Mar ...	Cisco360078	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.48 at Mar ...	Cisco360070	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.34 at Mar ...	Cisco360056	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.25 at Mar ...	Cisco360047	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.234 at Mar...	Cisco3600256	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.225 at Mar...	Cisco3600247	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.200 at Mar...	Cisco3600222	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.145 at Mar...	Cisco3600167	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.146 at Mar...	Cisco3600168	Router	UnAssigned	Critical	92 days ago	Like
<input type="radio"/>	NCM Script Execution operation failed for 6.1.1.132 at Mar...	Cisco3600154	Router	UnAssigned	Critical	92 days ago	Like

Enterprise Edition – 분산 처리 구성



NCM의 Enterprise Edition은 Central-Probe 분산 아키텍처를 통해 원격 위치의 장치에 대해서 모든 구성 작업을 수행할 수 있습니다.

구성을 중앙에서 관리하고, configlet을 실행하고, 여러 위치에 있는 모든 개별 Probe에서 다양한 구성 작업을 예약할 수 있습니다!

Networking 도구

Tools	Settings
Terminal (SSH/TELNET)	
Ping Tools	
Address Monitoring	
Network Monitoring	
SNMP Tools	
Cisco Tools	
Workflow	>
Forward Syslog	
Syslog Viewer	

Telnet/SSH 프로토콜에 대한 명령 구성 및 실행.

Ping을 사용하여 장치 도달 가능성 확인.

SNMP 도구를 사용하여 SNMP 그래프 표시.

주소 모니터링을 통해 MAC/DNS 찾기

syslog 메시지를 전달 및 수신

NCM의 장점

사용자 친화적!

NCM은 사용자 친화적인 GUI이며,
직관적인 다이얼과 그래프로 구성
변경 관리를 간단하고 쉽게 만듭니다.



토탈 패키지!

많은 네트워크 장치를 효과적으로

관리하여,

효율적인 작업 플랫폼으로 고객에게

완벽한 만족을 제공합니다.



감사합니다

텔리맨트 주식회사

<https://www.tmn.co.kr>

02) 588-7350

기술 질문: inforeq@tmn.co.kr

견적 요청: sales-info@tmn.co.kr