



Tivoli Netcool Configuration Management

Smarter Service Activation

Smarter Service Activation



- Network complexity and impacts
- What do we mean by Smarter Service Activation?
- Customer examples

The challenges facing Network Administrators

Network complexity raises operational costs

Increasing number of vendors and type of network devices

- Cisco, Juniper, Alcatel, Lucent, Nokia, Ericsson, Huawei, Motorola, NSN, Tellabs, etc.
- Routers, switches, DSLAMs, gateways, softswitches, IMS, LTE, SBCs, access points, fiber terminals, and more

Increasing network complexity

- 100's to 100,000's of devices deployed
 - Number of devices prevents any effective manual solution from being effective.
- Each network device vendor has multiple network element operating systems
 - There are over +400 network element vendors and divisions deployed in networks today
- Each network element model may have its own unique set of commands and version of OS
 - Command set changes with each OS version and each device supports from 10s to 10,000's of individual commands



The Impact of Network Complexity

Incorrect provisioning and excess inventory

35% of network assets lost or deployed erroneously

Network complexity outpacing scripting

60 average configuration errors per 1000 lines

Routine tasks consuming resources

45% of engineering time spent on manual config

Errors largest cause of network outages

60% caused by manual configuration errors

Inconsistent security posture open to threat

80% of security breaches from non-compliant devices

Sources: Dataquest, EMA, Yankee, Infonetics Research

The financial consequences

– Market Costs

- Time to Revenue - Time required to provision services in mins, days, weeks, months
- Customer acquisition - Time and resources spent determining if you can deliver services
- Customer Churn - Time and resources spent retaining customers and preventing churn

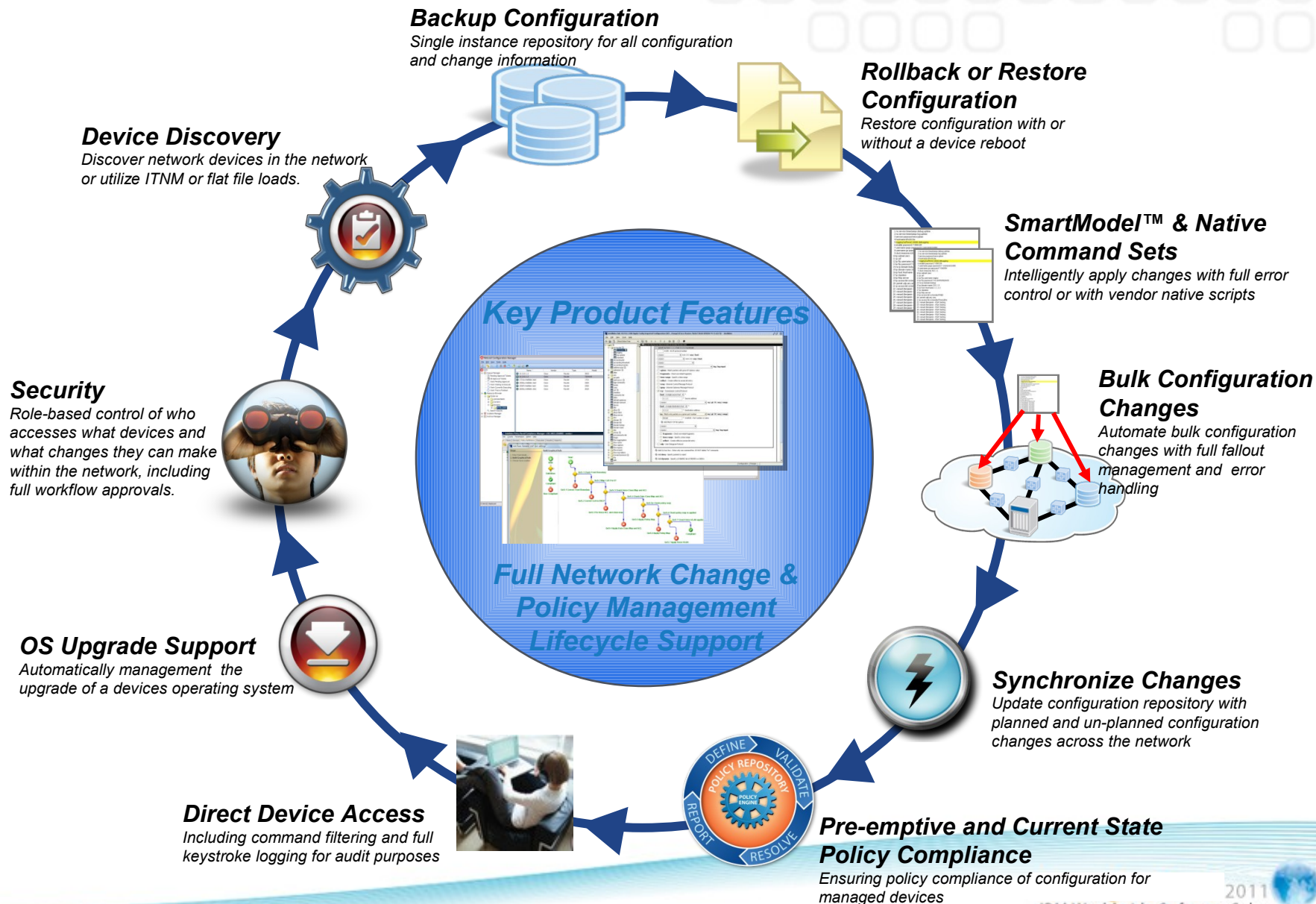
– Operations Costs

- Resources to Operate network
- Time to issue resolution

– Preventable costs

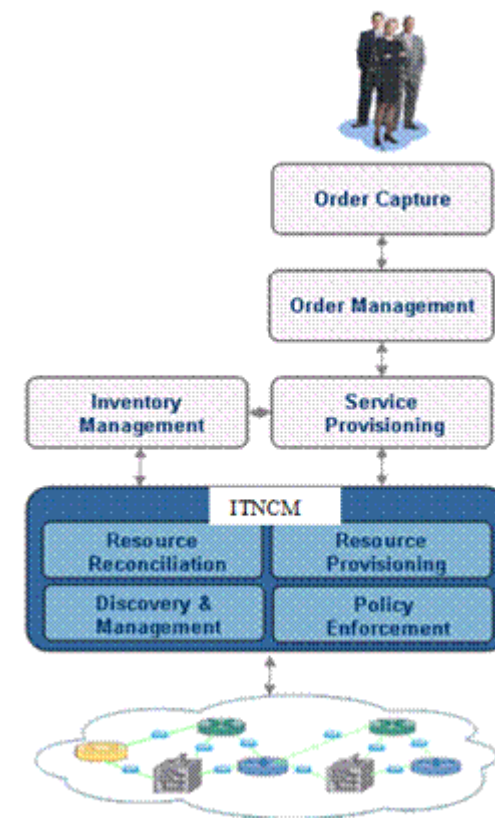
- Network Outages - Revenue per Customers impacted, transactions aborted, etc.
- SLA Penalties - Cost per miss, network uptime percentages, network availability

ITNCM: Intelligent Tool for Network Operations



Smarter Service Activation

- **Visibility** of the current state
 - Accurate “stateful” inventory & configuration model
 - Minimise stranded assets; “de-activation” supported
 - Get it right – first time
- **Control** of network compliance
 - Audit and Policy enforcement
- **Automate** to smooth the workflow
 - Powerful productivity tools
 - Integration with provisioning tools



IBM Tivoli Netcool Configuration Manager

Answers to your network complexity challenges

Reliable and Verifiable Change Automation

- Track every change on every device even the ones that didn't go through "official channels"
- Push out 1,000's of complex network changes and verify each change, every time.
- Build intelligent command sets with built in error checking and control
- Provide repeatable templates and processes that can be used with confidence

Network Security and Access Control

- Control who can access what device and what commands and parameters they can use.
- Maintain a complete log of all changes, including full two keystroke logs for terminals
- Build effective change authorization workflows to maintain effective control of the network

Comprehensive Network Back-up and Recovery

- Builds a comprehensive backup of all network devices through intelligent change monitoring
- Enables recovery through Roll-back to a previous state without impacting the service

Prevent Errors and Ensure Compliance

- Industry first with pre-emptive compliance, prevent problems before they occur
- Full policy engine to enforce standards, engineering mandates, and security

TNCM – Detailed Functional Map

Network Provisioning

'No-Scripts' Network Activation

State-Aware Provisioning with Device Dependent Checking and Automated Command Sets

Pre-Provisioning Validation of Commands, Order, and Violations

Operator and API driven Reusable Provisioning Templates

Full Support for Run-Time Parameters within Templates

Full Move, Add, Change, Delete Lifecycle Support

Automatic Error and Exception Handling

Extensive APIs for Integration with Service Provisioning & Inventory Applications

Configuration & Change Management

Always Accurate Configuration

Workflow automation of Approvals, Multiple Device Changes, and Reporting

Near-Real time State-Aware Configuration Management

Command Order, Syntax, and Semantic Validation of Changes

Telnet / FTP / SNMP Communication Support

Configuration Synchronization upon Changes, Manual, Time Scheduled , Time from Last Change, etc.

Full Device Configuration Backup with Versioning and Filtering

Non-Disruptive Rollback or Reload and Reset recovery

Out-of-Band Change Detection via Syslog Monitoring and Filters

Full Configuration Search & any Version to Version Diffs

Native and XML based Scripting and Command sets

Graphical and Command Line UI

Compliance & Audit

Always-on Compliance

Complete Operational, Security & Regulatory Policy Definition and Enforcement.

Automatic / Always-On Compliance

Centralized Policy Repository

Reusable Policy Framework

Graphical Drag-and-Drop Rules / Policy Design

Intelligent Remediation of Policy Violations

Telnet Terminal Bidirectional Keystroke Logging

Auditing of Full Configuration History

Out-Of-The-Box Policies and Examples

Automatic Reporting upon Violation

Security & Administration

Fine-Grained Security Control

Control Device Access by User or User Group Role

Control Command Access Down to Individual Parameter(s)

Authenticate Users Using Internal or Radius Server Integration

Organize Network Devices into Realms by Geography and by Logical Groups based on Use or Customer

Enforce Policies Specific to User Groups or Realms

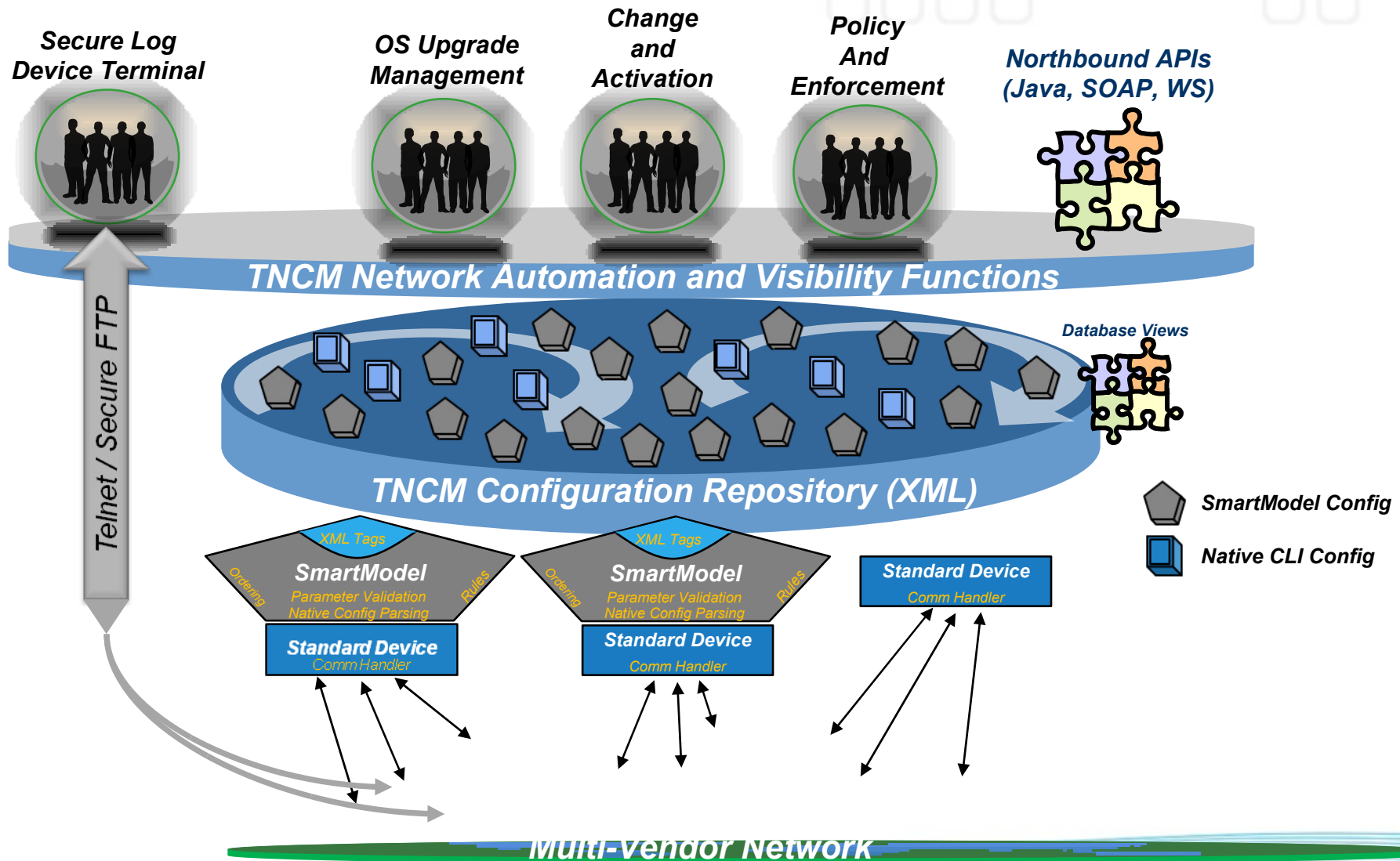
Creation of SNMP Events Upon Failure of any Security Authentication Failure

Centralized Group / Role / User Management

Track All Actions According to Group / Role / User levels

Track all User Activity both in System and Out of Band Changes

TNCM – Functional Architecture

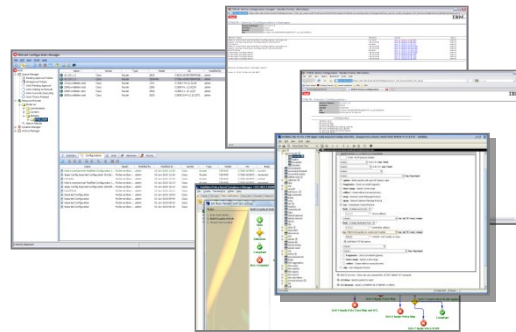


TNCM – Extensive Device Support Library

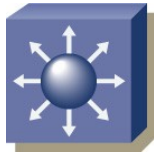


**Out-of-Box Support for over 850
Network Devices and
10,000's of OS Versions**

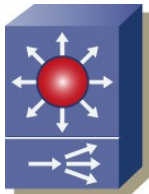
Tivoli Netcool Configuration Manager



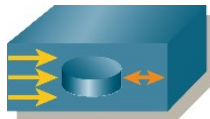
Multi-service
Switches



Content
Switches



WAN
Optimization



LAN Switches



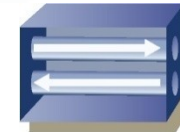
Routers



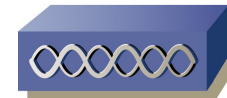
Firewalls



VPN
Concentrators



Wireless
Access
Points



Session Border
Controllers



Configuration modes

IBM Device Terminal (IDT)

```

# ip http server
# ip http secure-server

# ip forward protocol n
# route 0.0.0.0 0.0.0.0 18.216.1.254

# access-list extended WORDExtended
# permit tcp host 1.1.1.1 host 2.2.2.2 eq domain
# access-list extended word
# translate ruleent RULES from pad to telnet
# translate ruleent s from telnet to pad
# translate ruleent e from pad to telnet
# translate ruleent t from pad to telnet
# translate ruleent u from pad to telnet
# translate ruleent word from pad to telnet
# access-list word
# match cmd word xot-source-address word dest-address window-size word cli word na
# match cmd word dest-address window-size word na word
# match cmd word reversed word cli word dest-address word cli word xot-s
# access-list word
# match cmd word

```

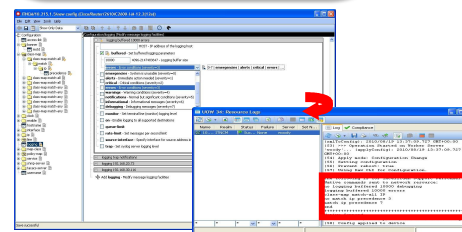
Native Commands

```

1 #
2 # This file is part of the Ansible
3 #
4 # Ansible is free software: you can redistribute it and/or modify
5 # it under the terms of the GNU General Public License as published by
6 # the Free Software Foundation, either version 3 of the License, or
7 # (at your option) any later version.
8 #
9 # Ansible is distributed in the hope that it will be useful,
10 # but WITHOUT ANY WARRANTY; without even the implied warranty of
11 # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
12 # GNU General Public License for more details.
13 #
14 # You should have received a copy of the GNU General Public License
15 # along with Ansible.  If not, see http://www.gnu.org/licenses/.
16 #
17
18 [defaults]
19 #log_path = /var/log/ansible.log
20 #log_level = INFO
21 #log_format = %b %p [%m]: %s
22 #log_formatter = ansible_log_formatter
23 #callback_whitelist = profile_tasks, profile_roles, profile_collections
24 #fork = 5
25 #local_timeout = 30
26 #remote_timeout = 30
27 #ssh_transfer_method = scp
28 #ssh_host_key_check = yes
29 #ssh_host_key_check_methods = sha256,sha256-cert,sha256-sk
30 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
31 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
32 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
33 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
34 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
35 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
36 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
37 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
38 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
39 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
40 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
41 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
42 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
43 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
44 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
45 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
46 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
47 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
48 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
49 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
50 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
51 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
52 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
53 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
54 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
55 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
56 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
57 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
58 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
59 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
60 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
61 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
62 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
63 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
64 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
65 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
66 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
67 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
68 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
69 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
70 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
71 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
72 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
73 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
74 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
75 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
76 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
77 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
78 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
79 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
80 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
81 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
82 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
83 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
84 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
85 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
86 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
87 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
88 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
89 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
90 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
91 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
92 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
93 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
94 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
95 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
96 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
97 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
98 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
99 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk
100 #ssh_key_check_methods = sha256,sha256-cert,sha256-sk

```

SmartModel™ Configuration



- ▶ Configuration mode for expert users, and for ad-hoc use
- ▶ Telnet / SSH based device access
- ▶ Full keystroke logging & archival
- ▶ Automatic configuration backup
- ▶ Maintains an audit trail of all sessions
- ▶ IDT Command Filtering:
 - ▶ Reduce device mis-configuration
 - ▶ Restrict users to execute damaging commands (e.g. reboot, reload)

- ▶ Configuration mode for expert & novice users, and for frequent changes
- ▶ Reusable native command sets (templates) with parameter support and comprehensive logging
- ▶ Multiple execution modes - ad-hoc, scheduled and recurring
- ▶ Role based access control

- ▶ “No-scripts” configuration mode (i.e. visually driven) for granular device control and maximum change accuracy
 - ▶ No coding, no scripting; key input fields auto-filled
 - ▶ Device syntax, semantics and ordering enforced
 - ▶ Changes validated against current configuration
- ▶ Command sets (templates) for frequent / bulk changes
- ▶ Command level access control
- ▶ Requires Configuration SmartModels



Unique to ITNCM



Additional value delivered by SmartModels

Easier to make & validate complex config changes

Easy to user interface, ensures users to not have to have a detailed knowledge of the network devices e.g. Command Ordering, parameter checking etc ...



Security

Control right down to command level access on managed devices

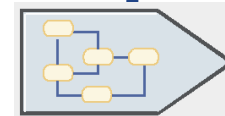
Report Only Mode

Check the impact of changes **before** applying them to the network.



De-provision correctly first time

The majority of inventory and configuration "ghosting" occurs during the de-provisioning process. SmartModels enable automatic, one-step de-provisioning

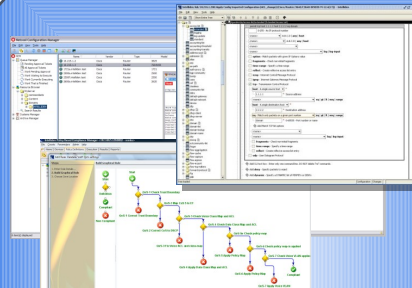


Intelligent Rollback

Restore previous configuration state **without** the need for device reboot



Tivoli Netcool Configuration Manager



Advanced Policy Compliance

Build and enforce complex policies across the network

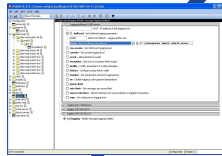
Improved Integration

Easing integrations to third party systems



Remove the need for scripting config changes

Dramatically reduce the expertise required to understand, define, and make changes to any device



Identify who made what changes when?

- Provides Netcool users with single-click access to ITNCM.
- Prebuilt TCR (Tivoli Common Reporting) reports which can be **launched in context** leveraging configuration data within OMNIbus and Network Manager.
- Helping to **diagnose problems quicker** resulting from configuration changes in the network.
- If permitted, Netcool users can perform configuration changes to resolve faults

The screenshot displays the Tenable Nessus web interface. At the top, there's a navigation bar with tabs for 'Tools', 'Hosts', 'History', 'Monitors', and 'Feed'. Below this, a search bar and a list of recent hosts are visible. The main section is titled 'Active Event List (AEL)' and contains a table of active events. The table has columns for 'Severity', 'Ack', 'Node', 'Alert Group', 'Summary', 'Last Occurrence', 'Count', 'Type', and 'Expires'. The events listed include alerts for device operation, policy evaluation, and system updates. The bottom status bar indicates '0 rows loaded, 0 rows updated, and 0 rows deleted'.

Severity	Ack	Node	Alert Group	Summary	Last Occurrence	Count	Type	Expires
Info	No	7505b.intelnet.1	80 Application	Device operation on Device: 7505b.intelnet.test_ossu_router...	6/20/19 10:23 PM	1	Information	Not Set
Info	No	192.168.12.1	CDP-DEVICE	Device Information Received on Fanned-Out...	6/20/19 2:32 PM	2	Provision	Not Set
Info	No	192.168.20.30	30 Application	UOW 30 changed state to Finished...	6/20/19 2:37 PM	3	Type	Not Set
Info	No	192.168.20.1	1721a.intelnet	Policy evaluation on Device: 1721a.intelnet.test_ossu_router...	6/20/19 11:17 PM	19	Type	Not Set
Info	No	192.168.20.1	1607b.intelnet	Policy evaluation on Device: 1607b.test_ossu_router_10720s_C10705...	6/20/19 11:17 PM	8	Type	Not Set
Info	No	192.168.20.1	2050a.intelnet	Policy evaluation on Device: 2050a.intelnet.test_ossu_router...	6/20/19 11:15 AM	11	Type	Not Set
Info	No	192.168.20.1	80 Application	UOW 80 changed state to Unknown...	6/20/19 11:17 PM	19	Type	Not Set
Info	No	192.168.20.1	3640c.intelnet	Policy evaluation on Device: 3640c.intelnet.test_ossu_router...	6/20/19 11:17 PM	11	Type	Not Set
Info	No	192.168.20.1	2050a.intelnet	Policy evaluation on Device: 2050a.intelnet.test_ossu_router...	6/20/19 6:09 PM	3	Type	Not Set
Info	No	192.168.20.1	10215.1.intelnet	Policy evaluation on Device: 10215.1.4.4_ossu_router_2050c.0...	6/20/19 6:09 PM	3	Type	Not Set
Info	No	192.168.20.1	2500f.intelnet	Policy evaluation on Device: 2500f.intelnet.test_ossu_router...	6/20/19 6:09 PM	3	Type	Not Set
Info	No	192.168.20.1	831a.intelnet	Policy evaluation on Device: 831a.intelnet.test_ossu_router_3...	6/20/19 6:09 PM	3	Type	Not Set
Info	No	192.168.20.1	10215.1.intelnet	Policy evaluation on Device: 10215.1.2.1_ossu_router_22940c.0...	6/20/19 2:30 PM	1	Type	Not Set
Info	No	192.168.20.30	30 Application	UOW 30 changed state to Finished...	6/20/19 2:40 PM	3	Type	Not Set
Info	No	192.168.20.1	7505b.intelnet	Policy evaluation on Device: 7505b.intelnet.test_ossu_router...	6/20/19 6:09 PM	2	Type	Not Set
Info	No	192.168.20.30	10215.1.intelnet	Policy evaluation on Device: 10215.1.3.3_ossu_router_22940c.0...	6/20/19 2:40 PM	3	Type	Not Set

Last 'n' device changes & when?

ITNCM: Device Configuration

Device Name	Vendor	Model	ID
10.215.1.3	Cisco	7200-VXR	C7200-ADVENTERPRISEK9-M-12.2(33)SRD3

Work Type

Native command set Modified Configuration (NoCDRun)	Status	Date	User
Apply Config Imported Configuration (NoCDRun)	current	Jun 2, 2010 1:39:20	admin
Firmware	locked	Jun 2, 2010 1:39:20	admin
Native command set Modified Configuration (NoCDRun)	locked	Jun 2, 2010 1:39:20	admin
Apply Config Imported Configuration (NoCDRun)	versioned	Jun 2, 2010 1:39:20	admin
NoCDRun	versioned	Jun 2, 2010 1:39:20	admin
Imported Configuration	versioned	Jun 2, 2010 1:39:20	admin

Configuration detail report

ITNCM: Device Configuration

Device Name	Vendor	Model	ID
10.215.1.3	Cisco	7200-VXR	C7200-ADVENTERPRISEK9-M-12.2(33)SRD3

Device terminal audit log

ITNCM: Device Terminal Audit Log

Start Time	Event Type	Keyboard Input	Device Output	User ID	Device Protocol
Jun 1, 2010 1:59 PM	DOT_CONNECT			admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		User Access Verification	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		Username: jopg	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		Password:	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DISCONNECT		% Login invalid	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_CONNECT			admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		User Access Verification	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		Username: gp	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_DEVICE_OUTPUT		Password:	admin	TelNET
Jun 1, 2010 1:59 PM	DOT_KEYBOARD_INPUT	config t	#%7200&term len 0	admin	TelNET
Jun 1, 2010 2:00 PM	DOT_DEVICE_OUTPUT		#%7200&term width 100	admin	TelNET
Jun 1, 2010 2:00 PM	DOT_KEYBOARD_INPUT	show cdp	% Invalid input detected at "^^" marker.	admin	TelNET
Jun 1, 2010 2:00 PM	DOT_DEVICE_OUTPUT		#%7200&config>exit	admin	TelNET

Device Unit of Work (UOW) Summary

ITNCM: Device Unit of Work summary

Device Name	Vendor	Model	ID
10.215.1.3	Cisco	7200-VXR	C7200-ADVENTERPRISEK9-M-12.2(33)SRD3

UOW ID	Task ID	UOW Description	User Description	Start Time	End Time	Task Result	User
UOW-13	1310ea000	Import Configuration	uuuu	Jun 1, 2010 9:22 AM	Jun 1, 2010 9:23 AM	Success	admin
UOW-14	1310ea000	Import Configuration	9999	Jun 1, 2010 9:39 AM	Jun 1, 2010 9:40 AM	Failure	admin
UOW-15	1510ea000	Import Configuration	lll	Jun 1, 2010 10:04 AM	Jun 1, 2010 10:04 AM	Success	admin
UOW-16	2010ea000	Configuration Change	kkkk	Jun 1, 2010 10:09 AM	Jun 1, 2010 10:09 AM	Failure	admin
UOW-17	2110ea000	Configuration Change	[REQ:Out]: Originally UOW#251 mrr	Jun 1, 2010 10:11 AM	Jun 1, 2010 10:12 AM	Success	admin
UOW-18	2210ea000	Native Command Set	PBCH Remedial Action - Policy: Cisco Discovery Protocol Disabled	Jun 1, 2010 10:13 AM	Jun 1, 2010 10:15 AM	Success	admin
UOW-19	3510ea000	Configuration change	changed for dedno	Jun 2, 2010 1:35 PM	Jun 2, 2010 1:37 PM	Success	admin
UOW-20	3610ea000	Native Command Set	PBCH Remedial Action - Policy: Cisco Discovery Protocol Disabled	Jun 2, 2010 1:38 PM	Jun 2, 2010 1:39 PM	Success	admin
UOW-21	810ea000	Import Configuration	Imported Configuration for AutoDiscovery	Jun 1, 2010 1:58 PM	Jun 1, 2010 1:16 AM	Success	admin

Displays a list of Units of Work and Tasks on this device grouped by UOW

Success Failure Dequeued S Single R Multiple

June 3, 2010 9:59:02 AM BST

1 /

ITNCM - Physical Asset Management

- Asset Management in a changing network is a major challenge for IT and Finance
 - Tracking what devices are currently in the network and what software features and loads are in production is the basis for equipment provider maintenance charges.
 - Typically NEPs charge customers for all the equipment purchased and all the software loads delivered regardless of what is actually deployed in the network, unless the customer agrees to an extensive audit, usually at their cost.
- ITNCM automatically builds a complete list of network assets each time it synchronizes with the network.
 - A standard ITNCM function is to synchronize device types, serial numbers, software versions, etc, and even provisioned features for each device and their associated cards or modules. This functionality is generally supported by most current network devices as this information is commonly stored as part of the device config.
 - A simple report can be built in ITNCM to provide end-users with enough detailed information to save \$100K's to \$1mlns in maintenance bills, by presenting NEPs with a detailed in service device report.
 - The updated physical asset information can also be uploaded into a dedicated asset management, like Maximo, or financial system like Oracle or SAP for tracking analysis through the ITNCM standard APIs.

TNCM – Representative Customers

<u>Customer</u>	<u>Business</u>	<u>Applications</u>	<u># of Devices</u>
	UK CSP; Leading Global MSP	Config., Compliance & Provisioning	+135,000
	US CSP and Managed Services Provider	Config., Compliance & Provisioning	+50,000
	Canadian CSP	Config, Compliance & Provisioning	+60,000
	Electrical Power Utility	Config. & OS Updates	+7,500
	Global Financial Transaction Company	Configuration & Compliance	+6,000
	Spanish and Latin American CSP	Core Configuration & Provisioning	+600
	Financial Institution in Canada	Configuration & Compliance	+1,500
	Italian CSP	Configuration & Compliance	+10,000
	ViaSat	Config, Compliance & Provisioning	+4,500
	Motorola	LTE Network Management	



BACKGROUND

**Leading US-based
Managed Services
Provider with ~42K SMB
Customers**

CHALLENGES

- Support aggressive growth plans – 3 new markets and 12K new customers per year
- Eliminate need for manual provisioning
- All-IP Cisco network
- Unlimited, carrier-class scalability not possible with existing internal solution
- ‘No-touch’ new service turn-up needed

Zero Touch Network Provisioning



**First-time ‘right’ provisioning
and minimized truck-roll**

TNCM Solution

- Network Provisioning, Configuration and Policy Management
- Unified solution for network engineering, operations and services teams

Deployment

- Devices: ~50K - Cisco IAD2400 Series (CPE) and 10,000 Series (aggregation) devices
- Users: ~160 Systems Engineers
- Supported Customers: 13 markets representing ~42K SMBs

Expected Results

- Minimize need to send installation technicians for CPE provisioning
- Shield CLI complexities from services / OSS teams
- Reduce ‘fat-finger’ configuration errors
- Control access i.e. who can do what and when
- Test provisioning changes before they are implemented
- Greater standardization
- Meet Customer SLAs





BACKGROUND

**Leading International
Credit Card Services
Provider**

CHALLENGES

- Highly visible, rapidly growing mission-critical financial network with 4000 Devices (95% Cisco)
- Prevent outages due to manual errors
- Reduce network OPEX growing linearly
- Scale the network engineering expertise ("tribal knowledge" syndrome)
- Consolidation of historically separate networks and management systems

Enhanced Automation, Accuracy and Audit



**75% time savings
through automation**

Solution

- Configuration & Change Management and reporting for IT audit group
 - IDT for unified access and control
 - Automated procedures for repetitive changes
 - Self-documenting workflow
 - OS Upgrades
- Integration with internal management web portal and inventory
- *Planning to integrate with Runbook automation and trouble ticketing applications*

Deployment

- Devices: ~4,000 (Cisco)
- Users: ~30 Systems Engineers
- Supported Customers: Internal IT Users across NA, LA, and Asia

Results

- Improved network reliability, greater automation, accuracy and audit
 - 50-60% changes automated with 75% time savings
 - 300 – 400 devices OS upgrades automatically saving two weeks' effort
- Lower TCO through reduced need for internal development and reduced hardware maintenance costs





BACKGROUND

**Managed Services
Provider to enterprises -
One of the world's most
advanced MPLS
networks with 28,000
ports in 170 countries**

CHALLENGES

- Provide an IP network with scale, resilience and security
- Accurately bid for new outsourcing contracts
- Meet stringent network availability & performance SLAs
- Ensure customer's network compliance obligations
- Reduce headcount to maintain multiple customer networks
- Reduce OPEX

MSP Configuration & Compliance



**300 Enterprises & 55K devices
operational in 6 months**

Solution

- Service assurance (part of BT's "trouble-to-resolve" process)
- Accuracy - "Getting things done right the first time"
- Business practices - "Single and consistent way of operating globally"
- System of record for all network changes
- Meet customer's network security & compliance obligations
- Ensures all devices within the networks meet's BT OS specifications
- Eliminates security threats posed by older OS releases

Deployment

- Devices: ~100K deployed; target ~500K devices
- Users: ~130 network engineers and support personnel
- Supported customers: >300 managed services enterprises (e.g. NHS, RBS, Reuters, Barclays, Ciba)

Results

- OPEX reduction
- Prevention of multiple SLA violations resulting in penalty reductions in the 100Ks GBP
- Prevention of customer down time
- Compliance remediation resulted in 10Ks of network changes to meet policy mandates

Summary – TNCM supporting smarter service activation

- Provides an accurate “as-is” database of record
- Activation is “right first time”
 - reduced drop-out
 - fewer stranded assets
- More rapid turnaround of activation cycle
 - flow-through
 - productivity tools to speed manual tasks



Thank You

