

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-5380C

Network Device Configuration Management with Oxidized and Bitbucket



PRESENTED BY

Adam Jacobs adajaco@sandia.gov



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Good Afternoon!

- Thanks for coming today!
- A little about me
- Ground rules

- The problem
 - Lots of devices
 - Lots of different *types* of devices
 - Lots of different people making changes on these devices
 - These people happen to be human beings
 - These devices have critical operational implications
 - These devices have critical security implications

How Sandia/California Used to Do It

- Network configurations were kept in a subversion repository
- Manual, error-prone process
 - Relied on network staff to replicate changes in two places
 - ... and to do it correctly, every time
 - ... and never to forget to do it
 - “But it’s just a small change. I’ll do it later!”
 - “I’m not sure we’re going to keep this change. I’ll do it later!”
- No reporting mechanism

What We Wanted

- New system that didn't have these problems
- Automatic detection, recording, and reporting of changes
- Changes detected in near real-time
- Easy way for staff to record comments about changes
- Easy way to pull configuration for rollbacks, if needed
- Had to work with a variety of vendors' equipment
 - We have Cisco, Arista, Juniper, Brocade, and Aruba
- Less expensive is better

What We Considered

- Solarwinds
 - Already in use for NPM
 - Seems to meet some of the requirements
 - I'm never really 100% happy with Solarwinds
- RANCID
 - Classic open-source tool for Cisco (and other) configuration management
 - Approximately 20 years old, still under active development
 - Whether its age is a good thing or a bad thing is personal opinion
 - Probably would have worked fine
 - Works on a polling-based "pull" model; no easy way to implement push

- oxidized
 - Newer (first released 2013) open-source alternative to RANCID
 - Does everything RANCID does, plus some extras
 - REST APIs
 - >120 supported device OSes (very easy to create new ones)
 - Written in ruby; easy to extend if you want
 - **Supports both push and pull for configuration changes**
 - Supports list-of-devices in a CSV file, a SQL database, or http url
 - Stores configurations in git, text file, or http POST
- oxidized is the backend worker that collects and stores all configuration changes. But we need a user-friendly tool to interact with that information.

- oxidized works best when it stores configurations in its git backend
- It can also be configured to do a “git push” to a remote repository on each detected configuration change
- This means any git GUI is a great accompaniment to oxidized
- We chose BitBucket, by Atlassian, for our front end, and it has worked out great.
 - Current Sandia policy makes storing configurations in the cloud difficult
 - BitBucket is available in both on-premise and cloud SaaS versions
 - Other git GUIs, like github or gitlab, would probably work too.
 - Absolutely can have the oxidized backend running locally, and the git GUI frontend on a different machine, including in the cloud.

How Do I Do It, and What Does It Cost?

- Installation is straightforward
 - oxidized: ruby gems, or docker
 - BitBucket: simple installer, or docker
- Configuration is also straightforward
 - Two configuration files for oxidized
 - List of devices to monitor
 - Short general configuration file
 - BitBucket has easy GUI-based configuration
- Easy on the wallet
 - oxidized is free (as in beer, and as in speech)
 - BitBucket
 - on-premise: \$10 for up to 10 users, reasonable pricing for more
 - SaaS: \$2/user/month
 - notifyr: optional extension but very helpful, on-premise only, \$10/10 users

Added Bonuses

- Device monitoring
- Looking at validation/compliance checking for future
- et cetera



Screen Shots



Change Notification Email

12

Bitbucket - Bitbucket Admin has pushed changes to Network Configs/Routers (master)



Bitbucket Admin (8554 Bitbucket) <8554-bitbucket@sandia.gov>

✓ Jacobs, Adam

Friday, May 10, 2019 at 14:39

[Show Details](#)



Bitbucket Admin has pushed changes to: 'master'

[Network Configs](#) / [Routers](#)

a6f05f3f461 update srn-core from 134. [REDACTED] criclar 10 May - 02:38 PM

M [srn-core](#)

```
177 177    !
178 178    !
179      - ! Last configuration change at 14:20:13 pdt Fri May 10 2019 by criclar
179      + ! Last configuration change at 14:38:47 pdt Fri May 10 2019 by criclar
180 180    ! NVRAM config last updated at 17:27:02 pdt Tue May 7 2019 by adajaco
181 181    !

2843 2843  ip route 10. [REDACTED] 255.255.255.255 204. [REDACTED]
2844 2844  ip route 10. [REDACTED] 255.255.255.255 204 [REDACTED]
2845      - ip route 10.199.0.0 255.255.128.0 134. [REDACTED]
2845      + ip route 10.198.0.0 255.255.128.0 134. [REDACTED]
2846 2846  ip route 134 [REDACTED] 255.255.0.0 Null0
2847 2847  ip route 134 [REDACTED] 255.255.254.0 134. [REDACTED]
```

You can [unwatch this repository](#) to stop receiving email updates.

Sent by [Notifyr for Bitbucket Server](#).



Repository View

13

The screenshot shows the Bitbucket interface for a repository named 'Network Configs / Routers'. The top navigation bar includes 'Bitbucket', 'Projects', 'Repositories', and 'Favourites'. A search bar is present with the text 'Search for code, commits or repositories...'. The left sidebar contains navigation icons for code, downloads, links, and settings. The main content area shows the repository path 'Network Configs / Routers' and a 'Watch' button. Below this, there is a 'Source' section with a dropdown menu set to 'master' and a breadcrumb 'Routers /'. There are 'Browse' and 'Filter' buttons. A table lists the repository's contents, including a folder 'hysterical-configs' and several files with their descriptions and last modified dates.

Source	Description	Last Modified
hysterical-configs		
asr10g-ES	update asr10g-ES	Yesterday
asr10g-L3	update asr10g-L3 from 134.	25 Apr 2019
asr4g-ES	update asr4g-ES	25 Apr 2019
asr4g-L3	update asr4g-L3 from 134..	25 Apr 2019
ca-dist	update ca-dist from ,	13 mins ago
ca-dist-new	update ca-dist-new from UnknownIpAddr	13 mins ago
dmz	update dmz	3 days ago
noobe	update noobe from 134.	Yesterday
outnet	update outnet from 134..	2 days ago
son-core	update son-core	2 days ago
srn-core	update srn-core from 134.	5 hours ago
voip-core.ca.sandia.gov	update voip-core.ca.sandia.gov	8 hours ago

Commits

14

Bitbucket Projects Repositories Favourites Search for code, commits or repositories...

Network Configs / Routers

Commits

master

Author	Commit	Message	Commit date
on	68cb39f3c69	update ca-dist from ...	15 mins ago
root	78d07294d0c	update ca-dist-new from UnknownIpAddr	16 mins ago
oxidized	85c4fca12e8	update ca-dist	2 hours ago
crclar	3b404fe3571	update srn-core from 134...	6 hours ago
crclar	a6f05f3f461	update srn-core from 134...	Q 1 6 hours ago
crclar	3a33fac46f1	update srn-core from 134...	6 hours ago
crclar	a0738ac4514	update srn-core from 134...	6 hours ago
crclar	138a9442311	update srn-core from 134...	Q 2 6 hours ago
oxidized	ee026f61bfb	update ca-dist	7 hours ago
oxidized	c09f01c3e5c	update voip-core.ca.sandia.gov	8 hours ago
adajaco	a66d41babc5	update ca-dist-new from 134...	9 hours ago
adajaco	6745d54950e	update ca-dist-new from 134...	9 hours ago
adajaco	ad9e1360951	update voip-core.ca.sandia.gov from 134...	9 hours ago

Commit #1

15

Bitbucket Projects Repositories Favourites Search for code, commits or repositories...

Commits

criclar committed `a6f05f3f461` 6 hours ago
update `srn-core` from 134.

`3a33fac46f1`
master
1 Participant
Download this commit
Unwatch this commit
No tags +

srn-core **MODIFIED** Blame


Adam Jacobs
This is a sample comment for my NLIT presentation
Reply · Edit · Delete · 12 mins ago

```
169 169 ! PID: WS-C6509-E-FAN      ,                VID: V04, SN: DCH162301GN
170 170 !
171 171 ! NAME: "PS 1 WS-CAC-6000W", DESCR: "AC power supply, 6000 watt 1"
172 172 ! PID: WS-CAC-6000W      ,                VID: V05, SN: AZS16280B7Q
173 173 !
174 174 ! NAME: "PS 2 WS-CAC-6000W", DESCR: "AC power supply, 6000 watt 2"
175 175 ! PID: WS-CAC-6000W      ,                VID: V05, SN: AZS16280B7V
176 176 !
177 177 !
178 178 !
179 - ! Last configuration change at 14:20:13 pdt Fri May 10 2019 by criclar
179 + ! Last configuration change at 14:38:47 pdt Fri May 10 2019 by criclar
180 180 ! NVRAM config last updated at 17:27:02 pdt Tue May 7 2019 by adajaco
181 181 !
182 182 version 15.2
```

Commit #2

Bitbucket Projects Repositories Favourites Search for code, commits or repositories...

Commits

 **criclar** committed `a6f05f3f461` 6 hours ago

update `srn-core` from 134.


`3a33fac46f1`
 master
 1 Participant
 Download this commit
 Unwatch this commit
 No tags +

srn-core **MODIFIED** Blame

```

169 169 | PID: WS-C6509-E-FAN      ,          VID: V04, SN: DCH162301GN
170 170 | !
171 171 | ! NAME: "PS 1 WS-CAC-6000W", DESCR: "AC power supply, 6000 watt 1"
172 172 | ! PID: WS-CAC-6000W      ,          VID: V05, SN: AZS16280B7Q
173 173 | !
174 174 | ! NAME: "PS 2 WS-CAC-6000W", DESCR: "AC power supply, 6000 watt 2"
175 175 | ! PID: WS-CAC-6000W      ,          VID: V05, SN: AZS16280B7V
176 176 | !
177 177 | !
178 178 | !
179 -  | ! Last configuration change at 14:20:13 pdt Fri May 10 2019 by criclar
179 +  | ! Last configuration change at 14:38:47 pdt Fri May 10 2019 by criclar

```

 **Adam Jacobs**
 Per-line comment
 Reply · Edit · Delete · A moment ago

```

180 180 | ! NVRAM config last updated at 17:27:02 pdt Tue May 7 2019 by adajaco
181 181 | !

```

Source View

17

The screenshot shows the Bitbucket web interface for a repository. The top navigation bar includes the Bitbucket logo, 'Projects', 'Repositories', and 'Favourites' menus, along with a search bar and utility icons. The left sidebar contains navigation icons for code, downloads, and other repository features. The main content area displays the 'Source' view for the file 'Routers / asr4g-ES' on the 'master' branch. The file content is shown in a monospaced font, detailing Cisco IOS XE software version 16.03.06 and various hardware specifications for an ASR1002-X chassis, including memory, processor, and power supply modules.

Bitbucket Projects Repositories Favourites Search for code, commits or repositories... ? ⚙️ 🏠 👤

Network Configs / Routers

Source

🔗 master ... Routers / asr4g-ES oxidized committed 1928f5efa1e 25 Apr 2019

Source view Diff to previous History Edit Blame Raw file

```
1 | Cisco IOS XE Software, Version 16.03.06
2 |
3 | Image: Software: X86_64_LINUX_IOSD-UNIVERSALK9-M, 16.3.6, RELEASE SOFTWARE (fc3)
4 | Image: Compiled: Wed 28-Feb-18 16:03 by mcpre
5 | Image: bootflash:asr1002x-universalk9.16.03.06.SPA.bin
6 | Chassis type: ASR1002-X
7 | Memory: main 1066313K/6147K
8 | Processor ID: FOX1841GPWA
9 | CPU: 2RU-X
10 | Memory: nvram 32768K
11 |
12 | VTP: show vtp status
13 |
14 | NAME: "Chassis", DESCR: "Cisco ASR1002-X Chassis"
15 | PID: ASR1002-X , VID: V02 , SN: FOX1841GPWA
16 |
17 | NAME: "Power Supply Module 0", DESCR: "Cisco ASR1002 AC Power Supply"
18 | PID: ASR1002-PWR-AC , VID: V03 , SN: ART1843U00M
19 |
20 | NAME: "Power Supply Module 1", DESCR: "Cisco ASR1002 AC Power Supply"
21 | PID: ASR1002-PWR-AC , VID: V03 , SN: ART1843U001
22 |
23 | NAME: "module 0", DESCR: "Cisco ASR1002-X SPA Interface Processor"
24 | PID: ASR1002-X , VID: , SN:
25 |
26 | NAME: "SPA subslot 0/1", DESCR: "1-port 10 Gigabit Ethernet Shared Port Adapter XFP based"
27 | PID: SPA-1X10GE-L-V2 , VID: V04 , SN: SAL18453YQP
```

Blame View

18

Source view Diff to previous History Edit **Blame** Raw file

Author	Commit Hash	Date	Line	Code
davshaw	2b432073386	08 May 2019	1421	switchport trunk allowed vlan 1-80,92-100,102-4094
mlkahn	a8c54746721	08 May 2019	1422	storm-control broadcast level 1.00
			1423	storm-control multicast level 1.00
			1424	!
davshaw	32e3624f1a2	18 Oct 2018	1425	interface Port-channel20
			1426	description Wireless Transport to DMZ Ten1/2 & Ten2/2
			1427	switchport
			1428	switchport trunk native vlan 99
			1429	switchport mode trunk
			1430	switchport trunk allowed vlan 300,301,350
davshaw	85e5e8a00e9	18 Oct 2018	1431	storm-control broadcast level 1.00
			1432	storm-control multicast level 1.00
			1433	!
davshaw	32e3624f1a2	18 Oct 2018	1434	interface Port-channel50
klam	ef2647870a7	28 Jun 2018	1435	description IP Phones
			1436	switchport
			1437	switchport mode trunk
adajaco	828431cabe1	08 May 2019	1438	switchport trunk allowed vlan 502-509
adajaco	84e726a68e8	08 May 2019	1439	storm-control broadcast level 1.00
klam	673da5ddca5	28 Jun 2018	1440	storm-control multicast level 1.00
			1441	!
klam	ef2647870a7	28 Jun 2018	1442	interface TenGigabitEthernet1/1
oxidized	93057e3603c	07 May 2018	1443	description Connects to ...
adajaco	e646219e20b	20 Jun 2018	1444	switchport
oxidized	93057e3603c	07 May 2018	1445	switchport mode access
			1446	switchport access vlan 201
adajaco	e646219e20b	20 Jun 2018	1447	storm-control broadcast level 1.00
oxidized	93057e3603c	07 May 2018	1448	storm-control multicast level 1.00
			1449	!
			1450	interface TenGigabitEthernet1/2
			1451	switchport
			1452	switchport mode access
			1453	switchport access vlan 43
			1454	shutdown
			1455	storm-control broadcast level 1.00
			1456	storm-control multicast level 1.00
			1457	!
			1458	interface TenGigabitEthernet1/3

Thank You!

Questions?

You can reach me later via email: adajaco@sandia.gov