Git Workflow to Manage Firewall Changes

Ryan Cresawn

College of Agriculture and Life Sciences

Proposal:

Use Git and Bitbucket as workflow tools to add change tracking and peer review to firewall change requests.

Counterargument 1:

Critique: New workflow will replace existing firewall change request methods.
Response: Proposed workflow is additive.

Counterargument 2:

Critique: New workflow imposes top-down authority structure.
Response: Maybe. Each College can impose any internal workflow they like.

Counterargument 3:

Critique: New workflow exposes firewall rule problems.
Response: Yes! Greater visibility of firewall rules is good.

MPLS:

2012-04: main campus project begins

Building firewalls removed.
College firewalls deployed.

2015-10: main campus project ends

Impact of AGG-MPLS on CALS net managers:

one-to-one: 1 net manager to 1.4 buildings
many-to-many: 10 net managers to 14 buildings

We're all in this together!

CALS MPLS buckets/firewall rule sets:

C-AGG (Computer Center)
AGG-MPLS (14 other buildings)

Firewall rules are text. They follow this pattern:

```
access-list Outside extended permit [protocol] [source] [destination]
[port]
```

These are firewall rules:

```
access-list Outside extended permit tcp host 128.196.150.28 host
150.135.41.48 object-group svc-winfs

access-list Outside extended permit tcp host 10.192.196.40 host
150.135.41.48 object-group svc-winfs

access-list Outside extended permit tcp host 128.196.156.115 host
150.135.41.48 object-group svc-winfs
```

These are prettier firewall rules:

```
object-group service database-services tcp
 description TCP ports for database services: MSSQL, MySQL, Redis
 port-object eq 1433
 port-object eq 3306
 port-object eq 6379

object-group network database-servers
 network-object host 10.140.110.6
 network-object host 10.140.110.5
 network-object host 128.196.199.133

object-group network database-clients
 network-object host 150.135.40.44

access-list Outside extended permit tcp object-group database-clients
object-group database-servers object-group database-services
```

Wikipedia definitions:

Git is a version control system that is used for software development and other version control tasks. As a distributed revision control system it is aimed at speed, data integrity, and support for distributed, non-linear workflows.

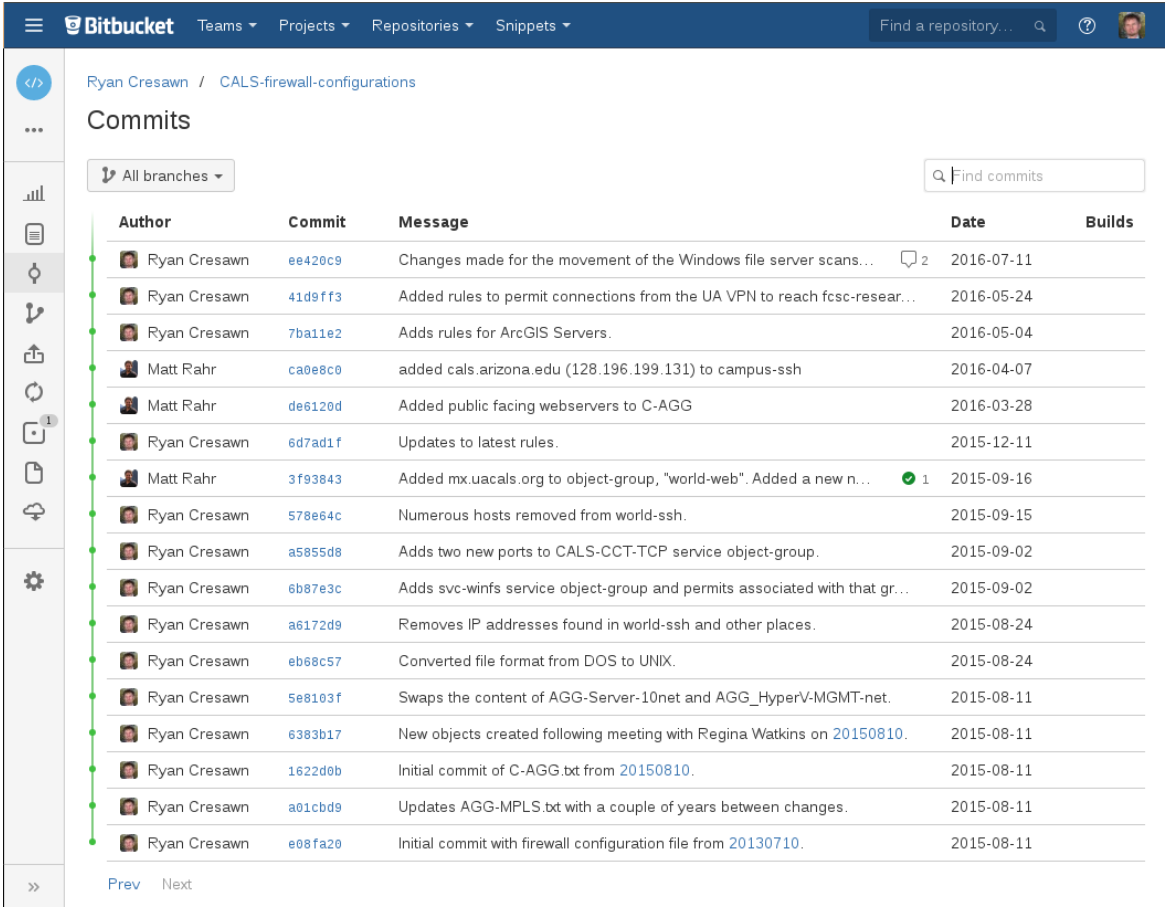
Bitbucket is a web-based hosting service for projects that use either the Mercurial (since launch) or Git (since October 2011) revision control systems.

The beginning (commit 1 of 77):

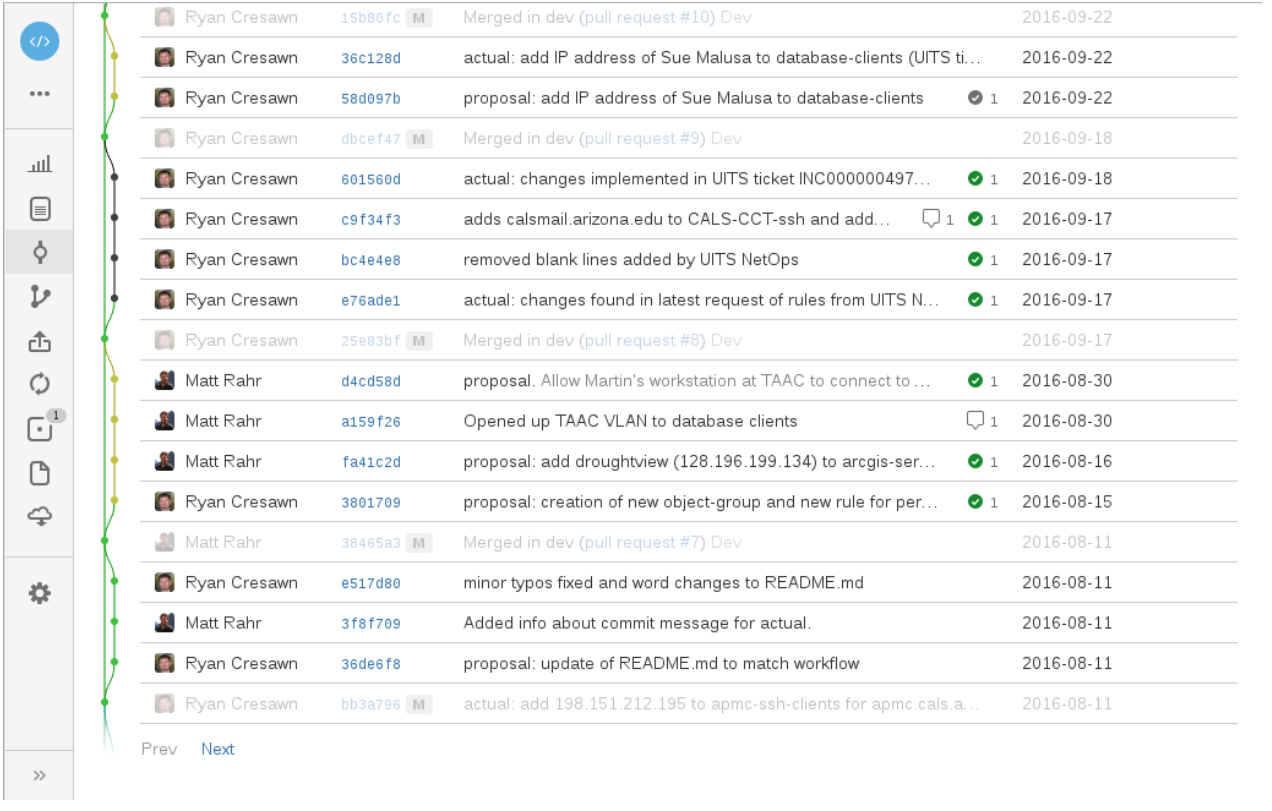
```
commit e08fa205de5713330b223b8c3098bec258d56119
Author: James Ryan Cresawn <*********@*****.***>
Date:   Wed Jul 10 11:46:39 2013 -0700

    Initial commit with firewall configuration
file from 20130710.
```

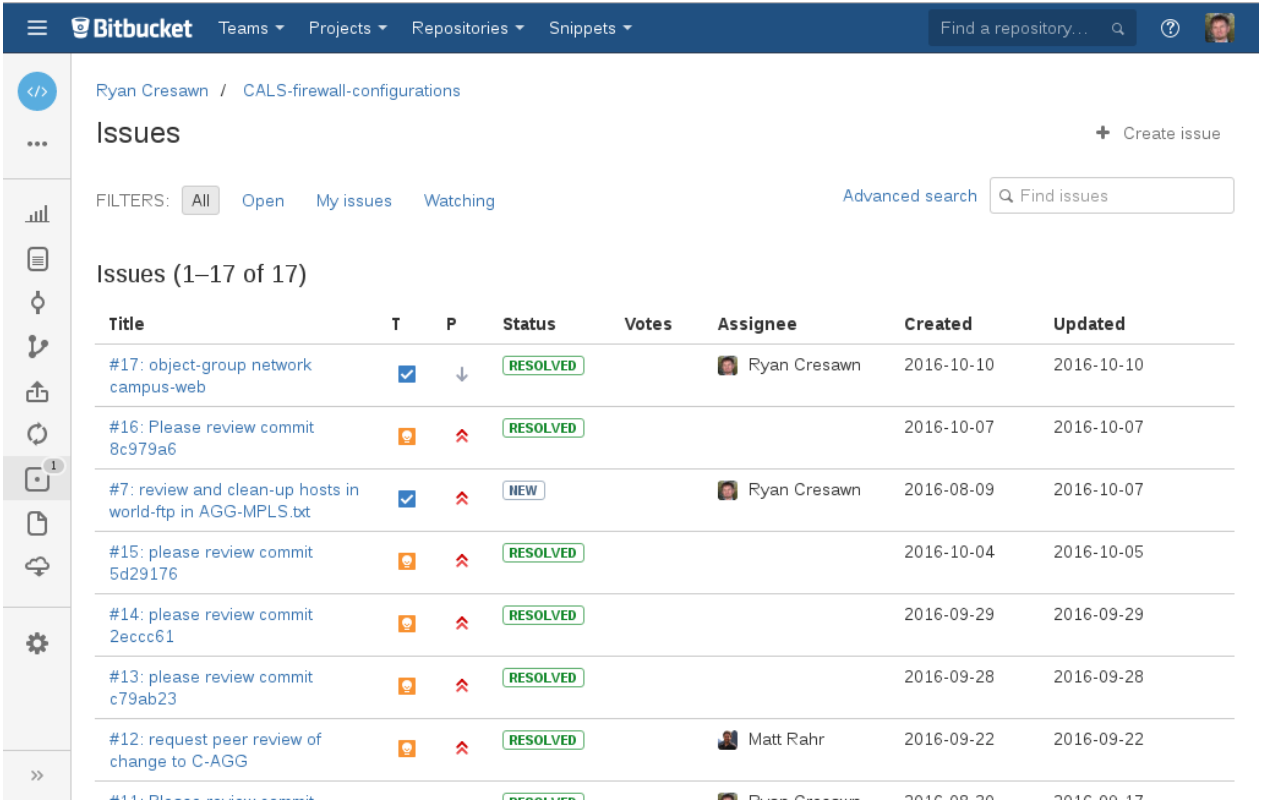
A pause (commit 2 of 77):

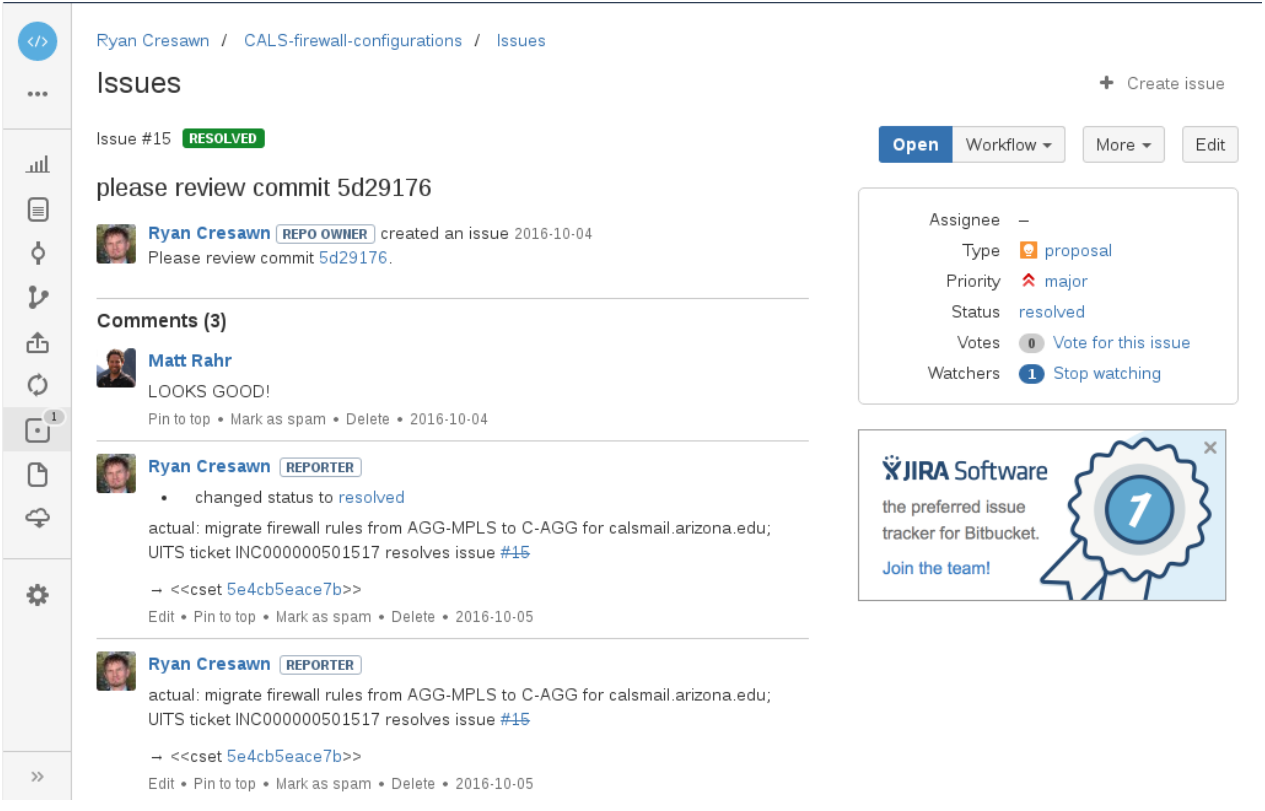
```
commit a01cbd963314a2f4483fb049ef2a530b1388f563
Author: James Ryan Cresawn <*********@*****.***>
Date:   Tue Aug 11 11:49:53 2015 -0700

    Updates AGG-MPLS.txt with a couple of
years between changes.
```

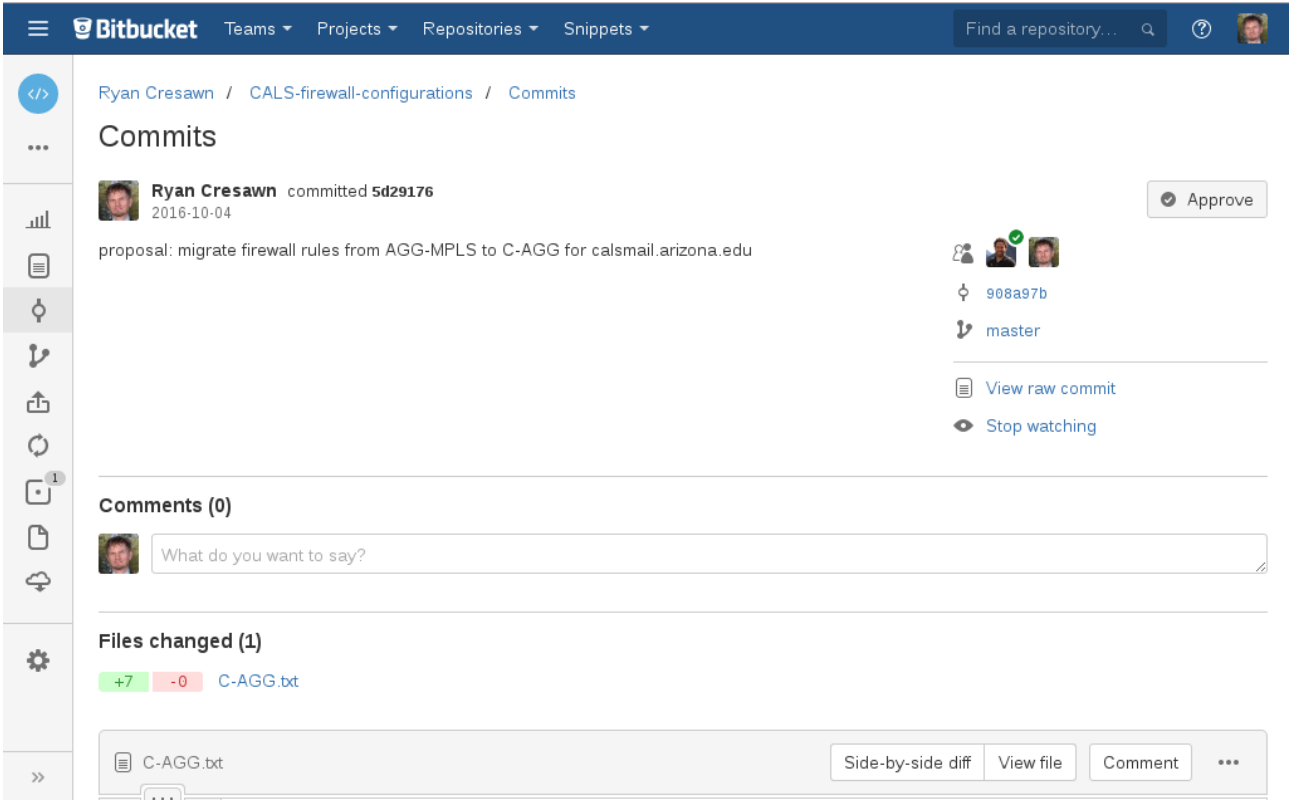

Bitbucket
Teams
Projects
Repositories
Snippets
Find a repository...
Ryan Cresawn / CALS-firewall-configurations
Commits
All branches
Find commits
Author
Commit
Message
Date
Builds
Ryan Cresawn ee420c9 Changes made for the movement of the Windows file server scans... 2 2016-07-11
Ryan Cresawn 41d9ff3 Added rules to permit connections from the UA VPN to reach fcsc-resear... 2016-05-24
Ryan Cresawn 7ba11e2 Adds rules for ArcGIS Servers. 2016-05-04
Matt Rahr ca0e8c0 added cals.arizona.edu (128.196.199.131) to campus-ssh 2016-04-07
Matt Rahr de6120d Added public facing webservers to C-AGG 2016-03-28
Ryan Cresawn 6d7ad1f Updates to latest rules. 2015-12-11
Matt Rahr 3f93843 Added mx.uacals.org to object-group, "world-web". Added a new n... 1 2015-09-16
Ryan Cresawn 578e64c Numerous hosts removed from world-ssh. 2015-09-15
Ryan Cresawn a5855d8 Adds two new ports to CALS-CCT-TCP service object-group. 2015-09-02
Ryan Cresawn 6b87e3c Adds svc-winfs service object-group and permits associated with that gr... 2015-09-02
Ryan Cresawn a6172d9 Removes IP addresses found in world-ssh and other places. 2015-08-24
Ryan Cresawn eb68c57 Converted file format from DOS to UNIX. 2015-08-24
Ryan Cresawn 5e8103f Swaps the content of AGG-Server-10net and AGG_HyperV-MGMT-net. 2015-08-11
Ryan Cresawn 6383b17 New objects created following meeting with Regina Watkins on 20150810. 2015-08-11
Ryan Cresawn 1622d0b Initial commit of C-AGG.txt from 20150810. 2015-08-11
Ryan Cresawn a01cbd9 Updates AGG-MPLS.txt with a couple of years between changes. 2015-08-11
Ryan Cresawn e08fa20 Initial commit with firewall configuration file from 20130710. 2015-08-11
Prev
Next

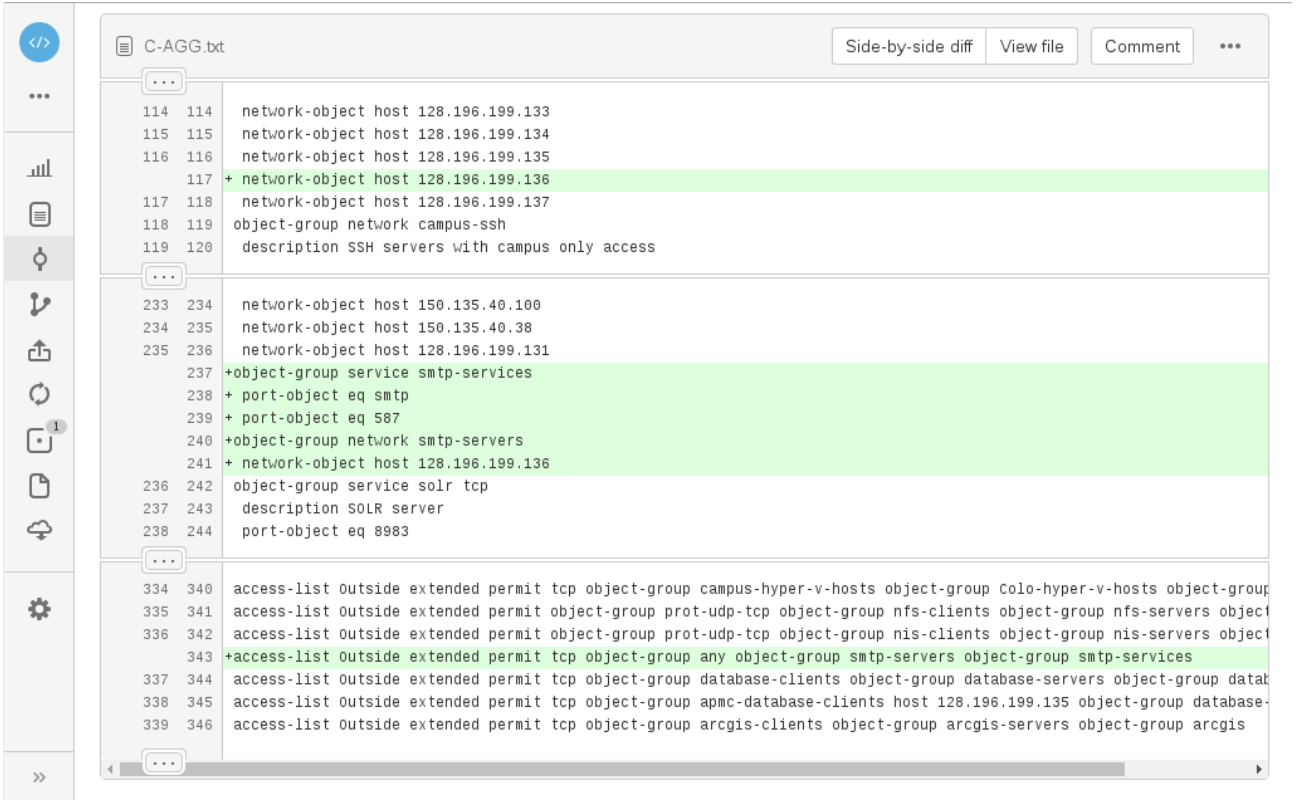
		2016-05-04
ampus-ssh		2016-04-07
		2016-03-28
		2015-12-11
eb". Added a new n...	1	2015-09-16
		2015-09-15
object-group.		2015-09-02
ts associated with that gr...		2015-09-02
other places		2015-08-24

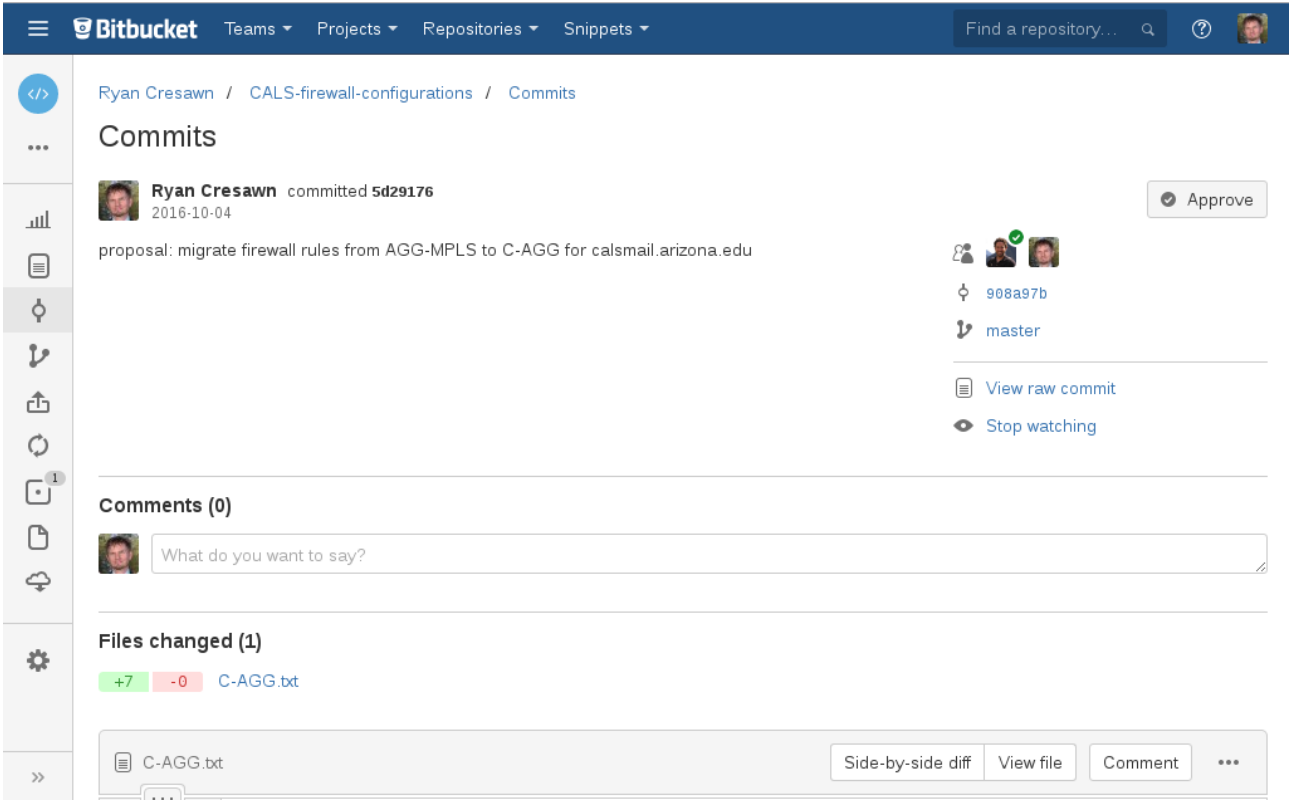

Ryan Cresawn 15b80fc M Merged in dev (pull request #10) Dev 2016-09-22
Ryan Cresawn 36c128d actual: add IP address of Sue Malusa to database-clients (UITS ti... 2016-09-22
Ryan Cresawn 58d097b proposal: add IP address of Sue Malusa to database-clients 1 2016-09-22
Ryan Cresawn dbcef47 M Merged in dev (pull request #9) Dev 2016-09-18
Ryan Cresawn 601560d actual: changes implemented in UITS ticket INC000000497... 1 2016-09-18
Ryan Cresawn c9f34f3 adds calsmail.arizona.edu to CALS-CCT-ssh and add... 1 1 2016-09-17
Ryan Cresawn bc4e4e8 removed blank lines added by UITS NetOps 1 2016-09-17
Ryan Cresawn e76ade1 actual: changes found in latest request of rules from UITS N... 1 2016-09-17
Ryan Cresawn 25e83bf M Merged in dev (pull request #8) Dev 2016-09-17
Matt Rahr d4cd58d proposal. Allow Martin's workstation at TAAC to connect to ... 1 2016-08-30
Matt Rahr a159f26 Opened up TAAC VLAN to database clients 1 2016-08-30
Matt Rahr fa41c2d proposal: add droughtview (128.196.199.134) to arcgis-ser... 1 2016-08-16
Ryan Cresawn 3801709 proposal: creation of new object-group and new rule for per... 1 2016-08-15
Matt Rahr 38465a3 M Merged in dev (pull request #7) Dev 2016-08-11
Ryan Cresawn e517d80 minor typos fixed and word changes to README.md 2016-08-11
Matt Rahr 3f8f709 Added info about commit message for actual. 2016-08-11
Ryan Cresawn 36de6f8 proposal: update of README.md to match workflow 2016-08-11
Ryan Cresawn bb3a796 M actual: add 198.151.212.195 to apmc-ssh-clients for apmc.cals.a... 2016-08-11
Prev
Next

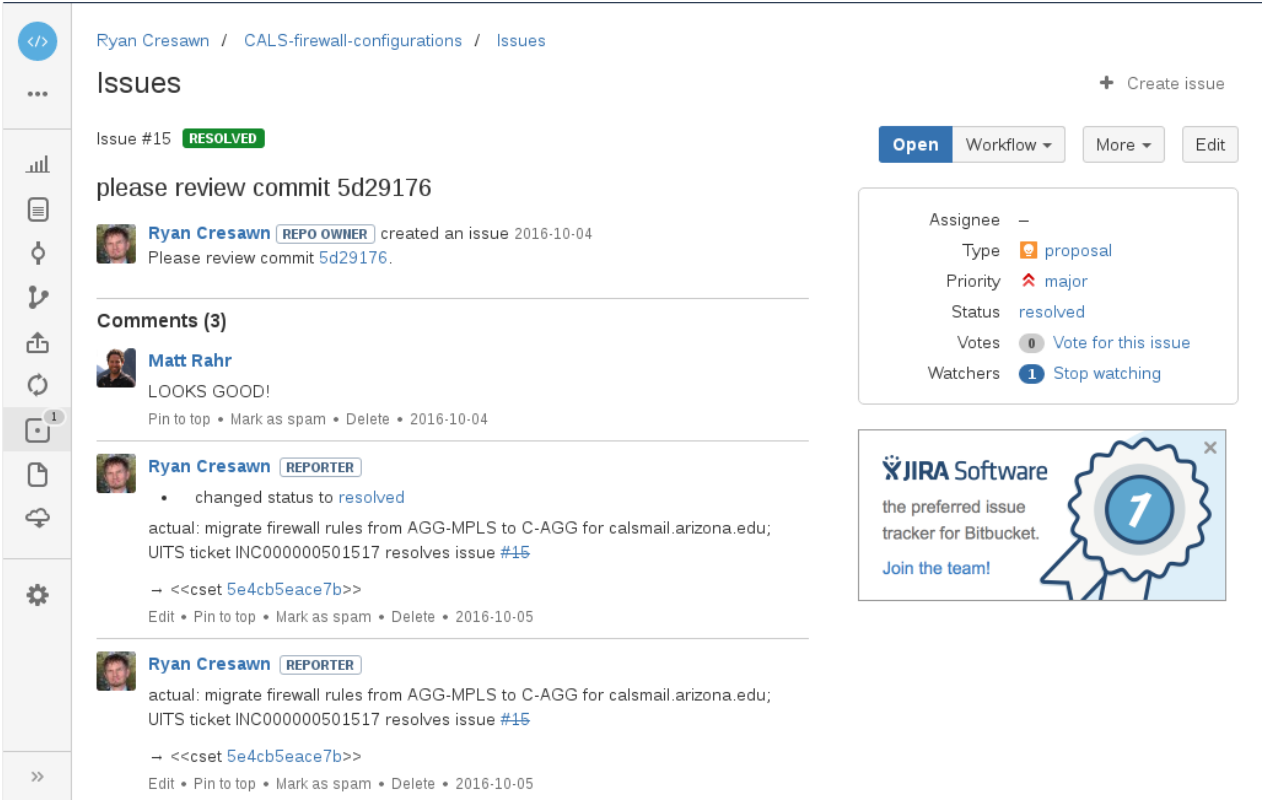

Bitbucket
Teams
Projects
Repositories
Snippets
Find a repository...
Ryan Cresawn / CALS-firewall-configurations
Issues
Create issue
FILTERS: All Open My issues Watching
Advanced search
Find issues
Issues (1–17 of 17)
Title T P Status Votes Assignee Created Updated
#17: object-group network campus-web RESOLVED Ryan Cresawn 2016-10-10 2016-10-10
#16: Please review commit 8c979a6 RESOLVED 2016-10-07 2016-10-07
#7: review and clean-up hosts in world-ftp in AGG-MPLS.txt NEW Ryan Cresawn 2016-08-09 2016-10-07
#15: please review commit 5d29176 RESOLVED 2016-10-04 2016-10-05
#14: please review commit 2eccc61 RESOLVED 2016-09-29 2016-09-29
#13: please review commit c79ab23 RESOLVED 2016-09-28 2016-09-28
#12: request peer review of change to C-AGG RESOLVED Matt Rahr 2016-09-22 2016-09-22


Ryan Cresawn / CALS-firewall-configurations / Issues
Issues
Create issue
Issue #15 RESOLVED
Open
Workflow
More
Edit
please review commit 5d29176
Ryan Cresawn REPO OWNER created an issue 2016-10-04
Please review commit 5d29176.
Assignee –
Type proposal
Priority major
Status resolved
Votes 0 Vote for this issue
Watchers 1 Stop watching
Comments (3)
Matt Rahr
LOOKS GOOD!
Pin to top • Mark as spam • Delete • 2016-10-04
Ryan Cresawn REPORTER
changed status to resolved
actual: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu; UITS ticket INC000000501517 resolves issue #15
→ <<cset 5e4cb5eace7b>>
Edit • Pin to top • Mark as spam • Delete • 2016-10-05
Ryan Cresawn REPORTER
actual: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu; UITS ticket INC000000501517 resolves issue #15
→ <<cset 5e4cb5eace7b>>
Edit • Pin to top • Mark as spam • Delete • 2016-10-05
JIRA Software
the preferred issue tracker for Bitbucket.
Join the team!


Bitbucket
Teams
Projects
Repositories
Snippets
Find a repository...
Ryan Cresawn / CALS-firewall-configurations / Commits
Commits
Ryan Cresawn committed 5d29176
2016-10-04
proposal: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu
Approve
908a97b
master
View raw commit
Stop watching
Comments (0)
What do you want to say?
Files changed (1)
+7
-0
C-AGG.txt
C-AGG.txt
Side-by-side diff
View file
Comment


C-AGG.txt
Side-by-side diff
View file
Comment
network-object host 128.196.199.133
network-object host 128.196.199.134
network-object host 128.196.199.135
+ network-object host 128.196.199.136
network-object host 128.196.199.137
object-group network campus-ssh
description SSH servers with campus only access
network-object host 150.135.40.100
network-object host 150.135.40.38
network-object host 128.196.199.131
+object-group service smtp-services
+ port-object eq smtp
+ port-object eq 587
+object-group network smtp-servers
+ network-object host 128.196.199.136
object-group service solr tcp
description SOLR server
port-object eq 8983
access-list Outside extended permit tcp object-group campus-hyper-v-hosts object-group Colo-hyper-v-hosts object-group
access-list Outside extended permit object-group prot-udp-tcp object-group nfs-clients object-group nfs-servers object
access-list Outside extended permit object-group prot-udp-tcp object-group nis-clients object-group nis-servers object
+access-list Outside extended permit tcp object-group any object-group smtp-servers object-group smtp-services
access-list Outside extended permit tcp object-group database-clients object-group database-servers object-group datab
access-list Outside extended permit tcp object-group apmc-database-clients host 128.196.199.135 object-group database-
access-list Outside extended permit tcp object-group arcgis-clients object-group arcgis-servers object-group arcgis


Bitbucket
Teams
Projects
Repositories
Snippets
Find a repository...
Ryan Cresawn / CALS-firewall-configurations / Commits
Commits
Ryan Cresawn committed 5d29176
2016-10-04
proposal: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu
Approve
908a97b
master
View raw commit
Stop watching
Comments (0)
What do you want to say?
Files changed (1)
+7
-0
C-AGG.txt
C-AGG.txt
Side-by-side diff
View file
Comment


Ryan Cresawn / CALS-firewall-configurations / Issues
Issues
Create issue
Issue #15 RESOLVED
Open
Workflow
More
Edit
please review commit 5d29176
Ryan Cresawn REPO OWNER created an issue 2016-10-04
Please review commit 5d29176.
Assignee –
Type proposal
Priority major
Status resolved
Votes 0 Vote for this issue
Watchers 1 Stop watching
Comments (3)
Matt Rahr
LOOKS GOOD!
Pin to top • Mark as spam • Delete • 2016-10-04
Ryan Cresawn REPORTER
changed status to resolved
actual: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu; UITS ticket INC000000501517 resolves issue #15
→ <<cset 5e4cb5eace7b>>
Edit • Pin to top • Mark as spam • Delete • 2016-10-05
Ryan Cresawn REPORTER
actual: migrate firewall rules from AGG-MPLS to C-AGG for calsmail.arizona.edu; UITS ticket INC000000501517 resolves issue #15
→ <<cset 5e4cb5eace7b>>
Edit • Pin to top • Mark as spam • Delete • 2016-10-05
JIRA Software
the preferred issue tracker for Bitbucket.
Join the team!

Workflow summary:

1. Create dev branch
2. Make changes in dev branch
3. Commit changes in dev branch
4. Push changes to Bitbucket
5. Create issue referencing commit ID
6. Wait for peer review/approval
7. Submit Remedy ticket, request export

8. Commit exported rules to dev branch

9. Merge dev into master, close dev, resolve issue

Proposal of new workflow:

- UITS Network Operations owns the repository
- CALS forks repository, make changes following internal peer review workflow
- CALS submits a pull request
- UITS Network Operations merges changes