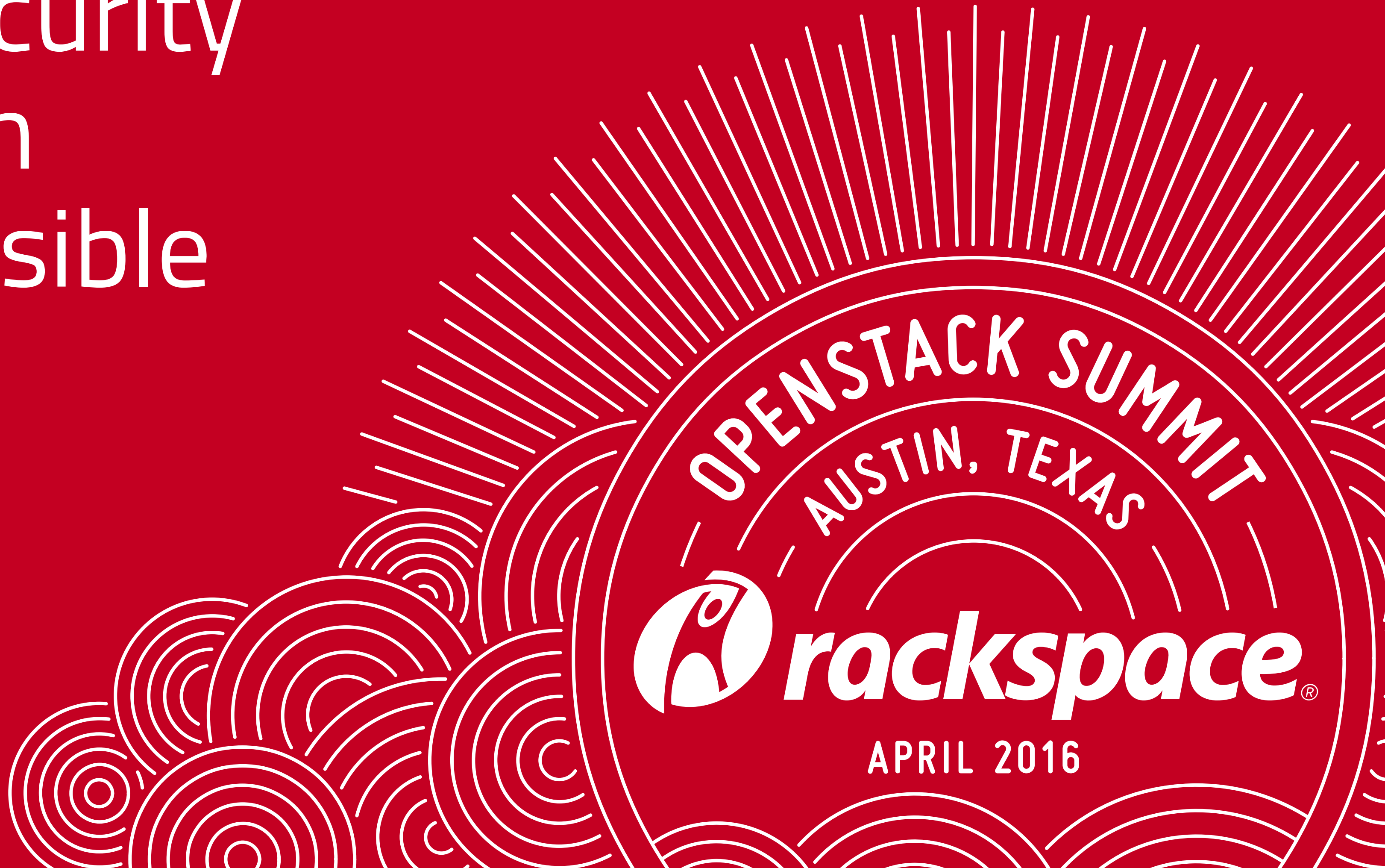
Automated Security Hardening with OpenStack-Ansible

Major Hayden

major.hayden@rackspace.com
@majorhayden



Major Hayden

Principal Architect

GIAC SECURITY ESSENTIALS CERTIFICATION GSEC

GIAC CERTIFIED UNIX SECURITY ADMINISTRATOR GCUX

RED HAT CERTIFIED ARCHITECT redhat

since 2006

since 2012

since 2011

Agenda

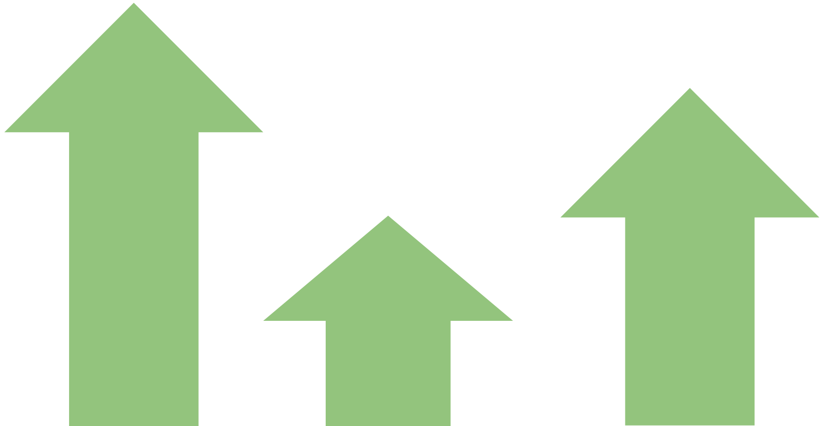
- Security tug-of-war
- Meeting halfway
- Get involved!

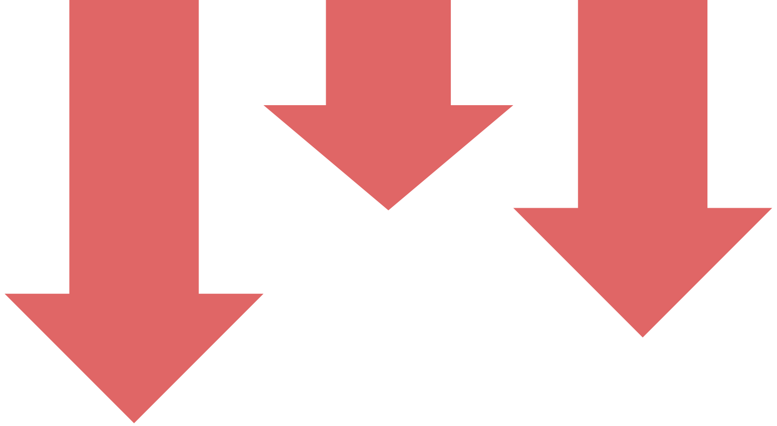
> We can all agree on one thing: information security is **insanely difficult**

We want just enough security

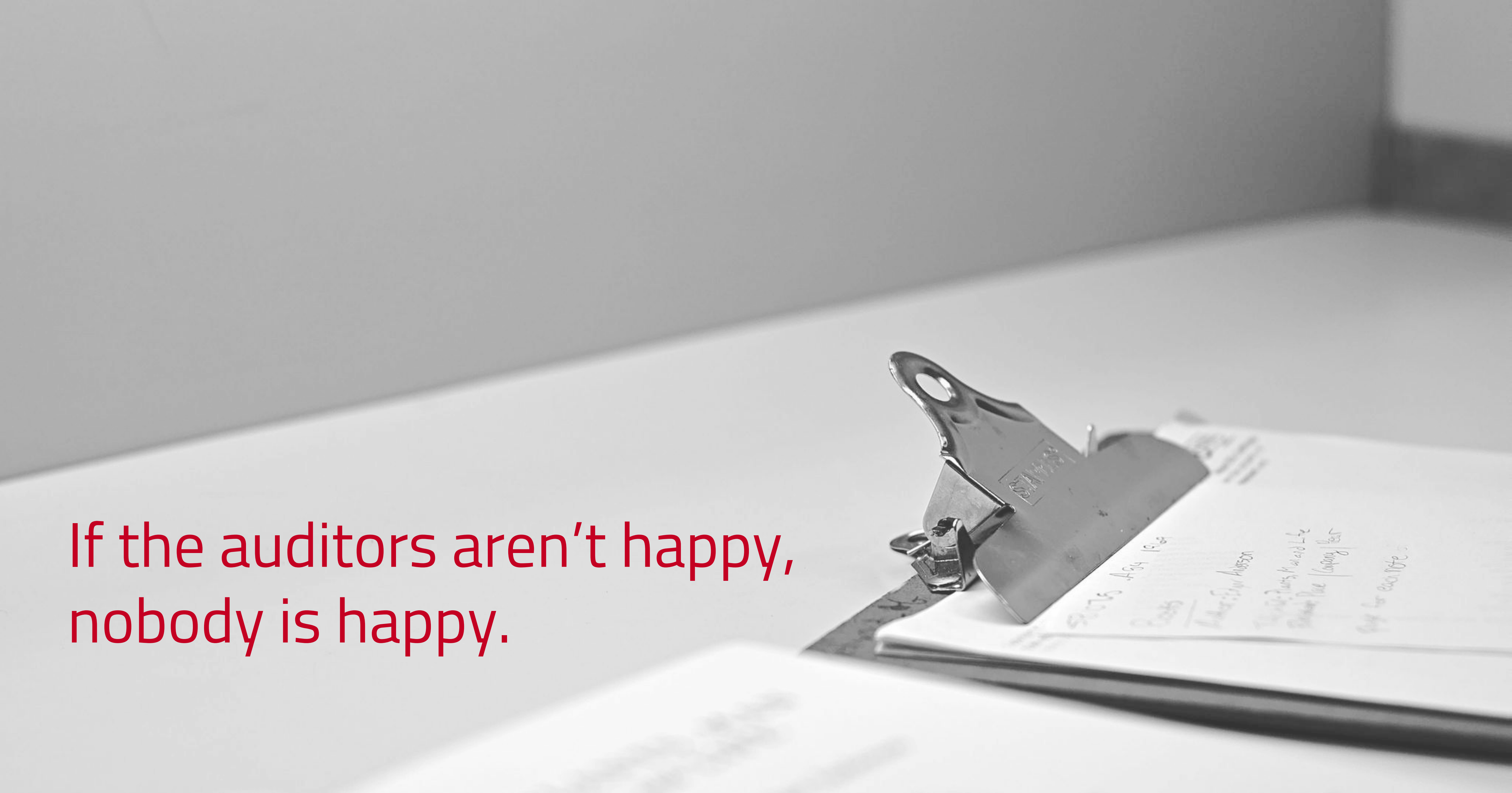
to create valuable outcomes

for our customers





We avoid security changes that **increase drag and friction** within our organizations



If the auditors aren’t happy,
nobody is happy.

Photo credit: Bruce Guenter (Flickr)

How do we make **valuable** security changes **without disruption** (and keep the auditors happy)?

Make security automatic

(And yes, I know that makes it sound easy.)

Photo credit: Jaime Walker (jw1697, Flickr)

> “When the going gets tough,
> the tough **adopt standards**”

(This isn’t a famous quote. I just made it up for these slides.)

Information security tip:

People should feel like security is something **they are a part of**; not something that is **being done to them**.

(I learned this lesson the hard way.)

Which sounds better?
Option #1

"As developers, you don't know how
to secure systems properly. We will tell you
what to do and you must have it done in three months.
If you don't, we can't take credit cards."

Which sounds better?
Option #2

“Since you use Ansible, we wrote some automation that fits into your existing deployment method and won’t disrupt your production environments.
Can we work with you to test it this month?”

Automated security for OpenStack must be:

Easy to implement

Simple to maintain

Non-disruptive to existing clouds

Effective against attacks

Open and transparent

PCI-DSS 3.1 Requirement 2.2:

“Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are **consistent with industry-accepted system hardening standards**.”

Selecting the right standard is challenging

Some are as long as novels

Very few directly apply to Ubuntu

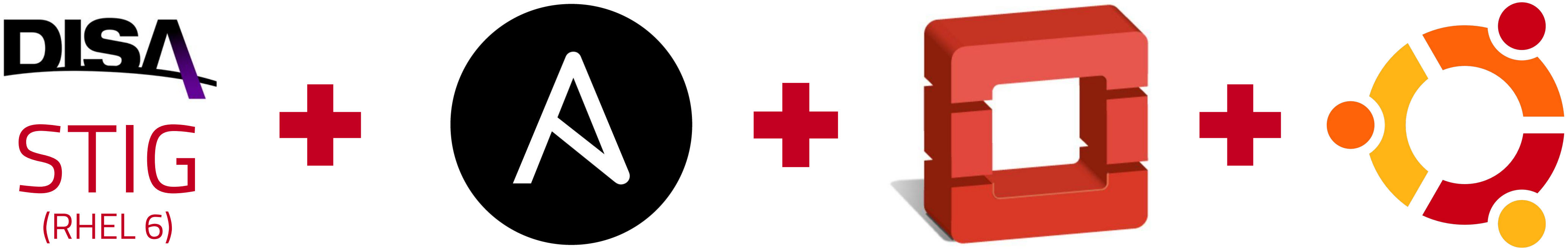
Some have restrictive licenses

Our selection:

Security Technical Implementation Guide (STIG)
from the Defense Information Systems Agency (DISA)

The STIG covers many of the most critical security domains

- Active services
- Authentication
- Boot-time security
- Consoles
- File permissions/ownership
- File integrity management
- Kernel tuning
- Mail
- Package management
- SSH daemon
- Syscall Auditing


DISA
STIG
(RHEL 6)
+
+
+

Ansible is a
software platform for
configuration management
and deployment
(among many other things)

OpenStack-Ansible deploys a **production-ready** OpenStack system using Ansible tasks and roles

OpenStack-Ansible has a security hardening role with two components:

Ansible Role

Applies automated security hardening to multiple systems

Documentation

With content for deployers as well as auditors

openstack-ansible-security role features:

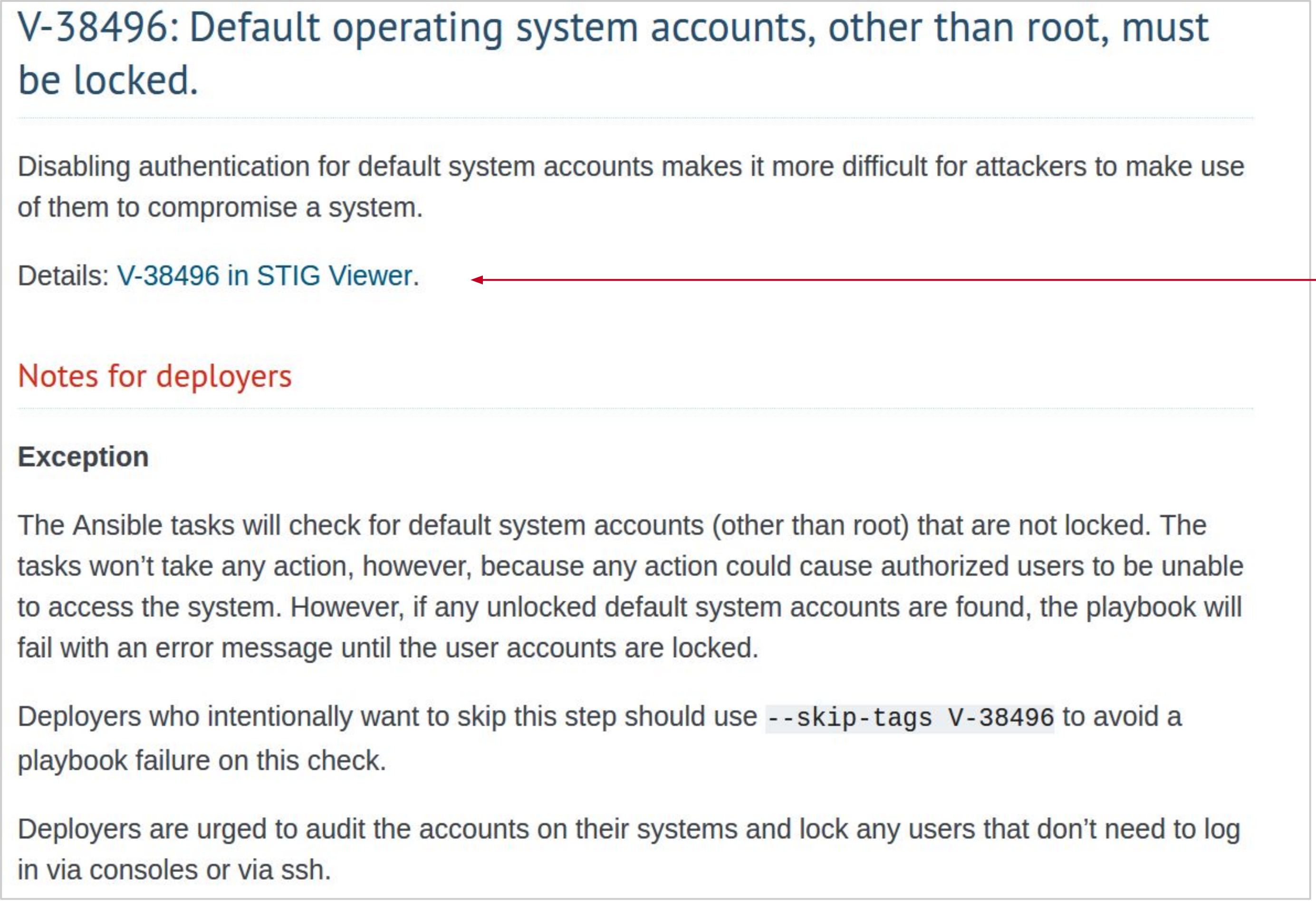
Applies **200+** security configurations in **90 seconds**

Highly configurable

Comes with a **built-in auditing mode** for testing or for use with compliance auditors

Carefully written to be **non-disruptive** to existing OpenStack clouds

Documentation



V-38496: Default operating system accounts, other than root, must be locked.

Disabling authentication for default system accounts makes it more difficult for attackers to make use of them to compromise a system.

Details: V-38496 in STIG Viewer.

Notes for deployers

Exception

The Ansible tasks will check for default system accounts (other than root) that are not locked. The tasks won't take any action, however, because any action could cause authorized users to be unable to access the system. However, if any unlocked default system accounts are found, the playbook will fail with an error message until the user accounts are locked.

Deployers who intentionally want to skip this step should use `--skip-tags V-38496` to avoid a playbook failure on this check.

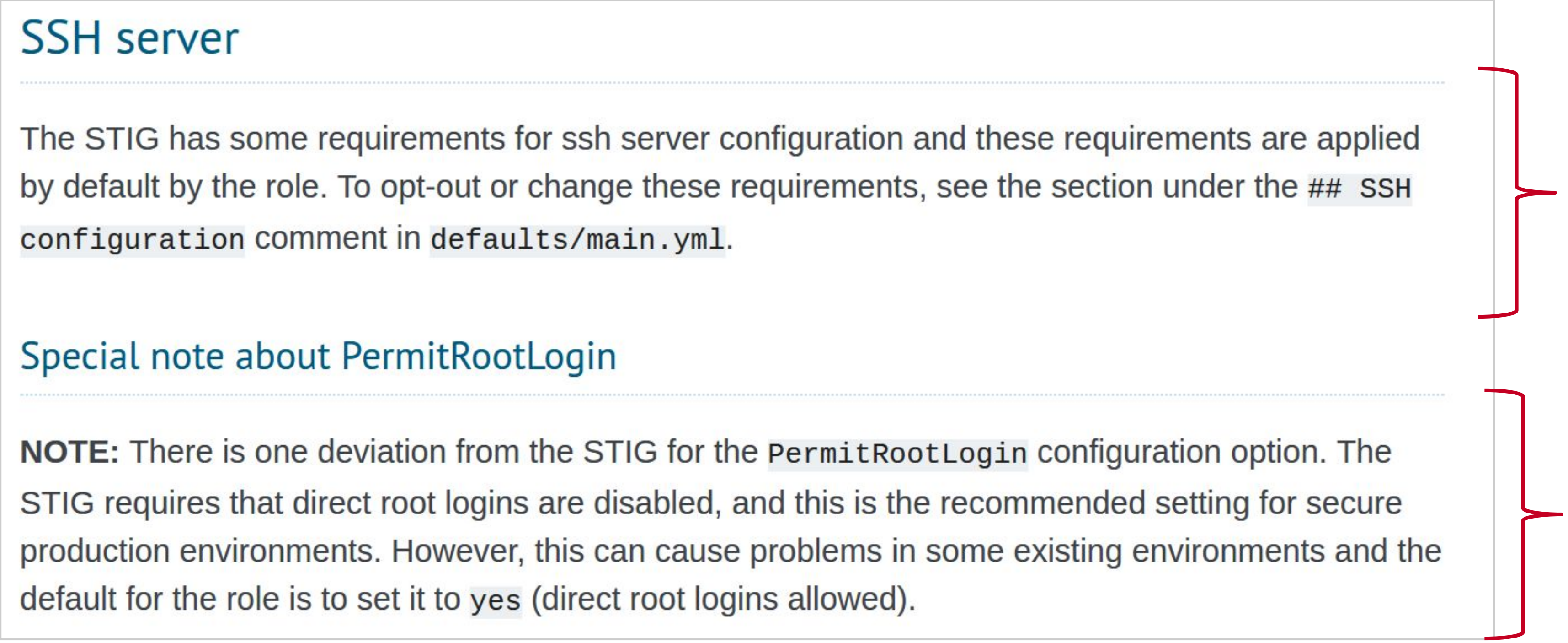
Deployers are urged to audit the accounts on their systems and lock any users that don't need to log in via consoles or via ssh.

Configuration requirement from the STIG

Link to the STIG viewer

Notes for deployers about exceptions and additional configurations
(auditors want to see these, too)

Documentation



SSH server

The STIG has some requirements for ssh server configuration and these requirements are applied by default by the role. To opt-out or change these requirements, see the section under the `## SSH configuration` comment in `defaults/main.yml`.

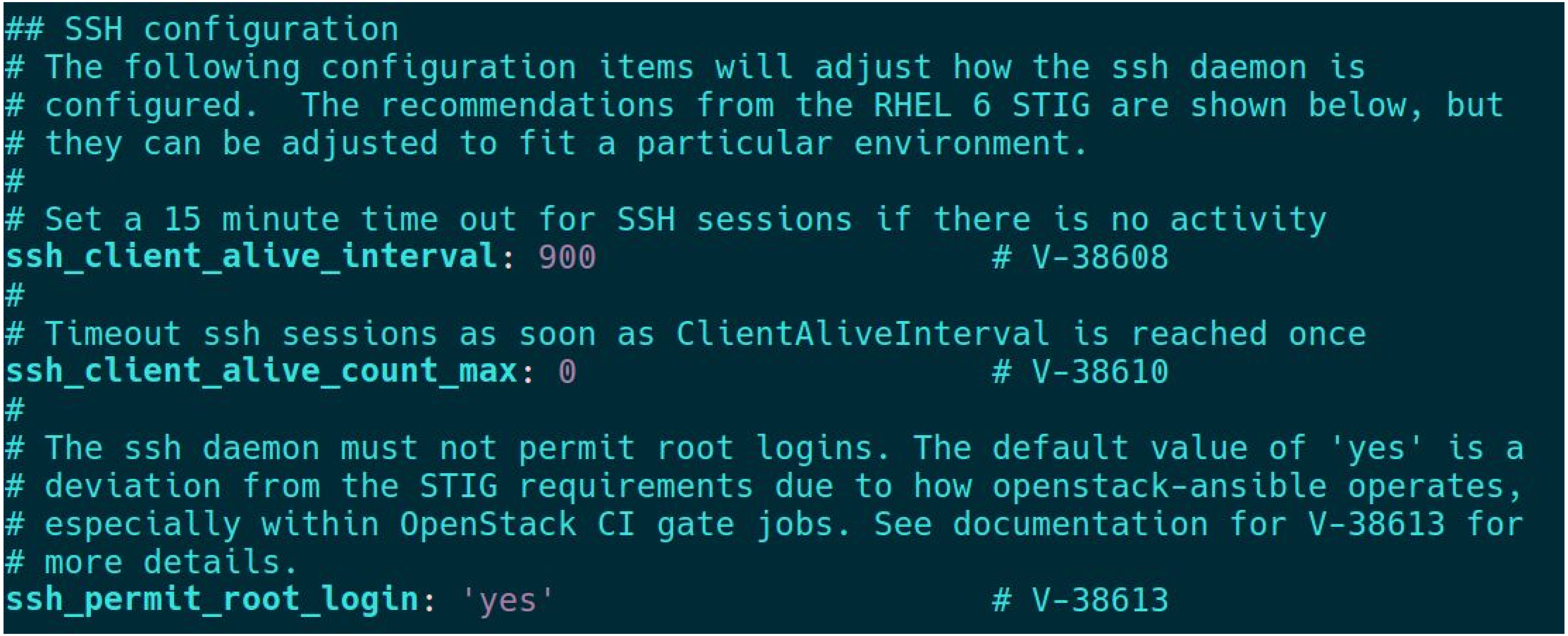
Special note about PermitRootLogin

NOTE: There is one deviation from the STIG for the `PermitRootLogin` configuration option. The STIG requires that direct root logins are disabled, and this is the recommended setting for secure production environments. However, this can cause problems in some existing environments and the default for the role is to set it to `yes` (direct root logins allowed).

References Ansible variable configuration options

Warnings and advice

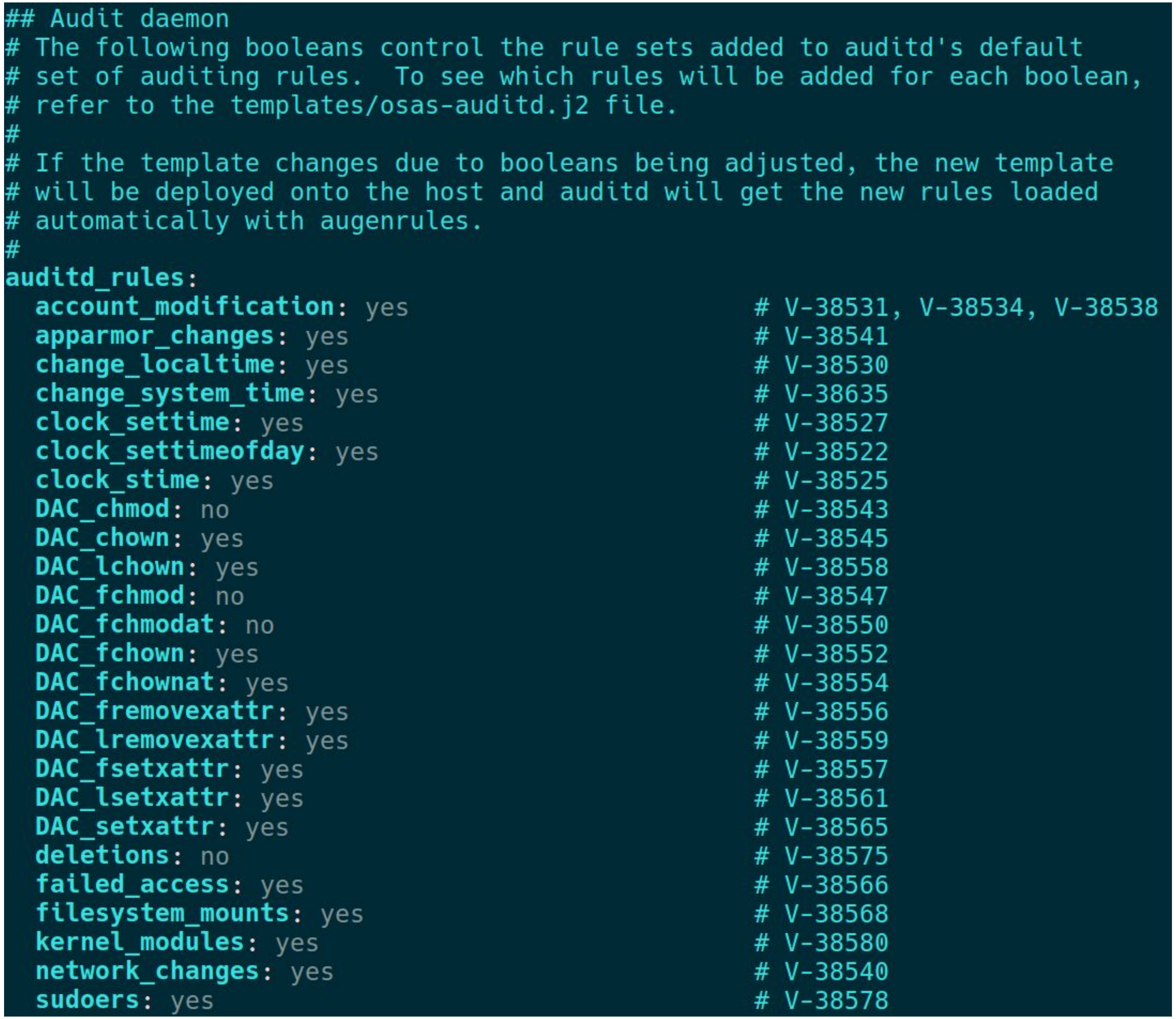
Configuration



```
## SSH configuration
# The following configuration items will adjust how the ssh daemon is
# configured.  The recommendations from the RHEL 6 STIG are shown below, but
# they can be adjusted to fit a particular environment.
#
# Set a 15 minute time out for SSH sessions if there is no activity
ssh_client_alive_interval: 900                    # V-38608
#
# Timeout ssh sessions as soon as ClientAliveInterval is reached once
ssh_client_alive_count_max: 0                     # V-38610
#
# The ssh daemon must not permit root logins. The default value of 'yes' is a
# deviation from the STIG requirements due to how openstack-ansible operates,
# especially within OpenStack CI gate jobs. See documentation for V-38613 for
# more details.
ssh_permit_root_login: 'yes'                      # V-38613
```

Configuration

Flip a boolean and redeploy the entire role or use a tag to only deploy certain parts.



```
## Audit daemon
# The following booleans control the rule sets added to auditd's default
# set of auditing rules.  To see which rules will be added for each boolean,
# refer to the templates/osas-auditd.j2 file.
#
# If the template changes due to booleans being adjusted, the new template
# will be deployed onto the host and auditd will get the new rules loaded
# automatically with augenrules.
#
auditd_rules:
  account_modification: yes                       # V-38531, V-38534, V-38538
  apparmor_changes: yes                           # V-38541
  change_localtime: yes                           # V-38530
  change_system_time: yes                         # V-38635
  clock_settime: yes                              # V-38527
  clock_settimeofday: yes                         # V-38522
  clock_stime: yes                                # V-38525
  DAC_chmod: no                                   # V-38543
  DAC_chown: yes                                  # V-38545
  DAC_lchown: yes                                 # V-38558
  DAC_fchmod: no                                  # V-38547
  DAC_fchmodat: no                                # V-38550
  DAC_fchown: yes                                 # V-38552
  DAC_fchownat: yes                               # V-38554
  DAC_fremovexattr: yes                           # V-38556
  DAC_lremovexattr: yes                           # V-38559
  DAC_fsetxattr: yes                              # V-38557
  DAC_lsetxattr: yes                              # V-38561
  DAC_setxattr: yes                               # V-38565
  deletions: no                                   # V-38575
  failed_access: yes                              # V-38566
  filesystem_mounts: yes                          # V-38568
  kernel_modules: yes                             # V-38580
  network_changes: yes                            # V-38540
  sudoers: yes                                    # V-38578
```

How do I get it?

OpenStack-Ansible deployers

Already available in OpenStack-Ansible's Liberty, Mitaka, and Newton releases!
Adjust *apply_security_hardening* to *True* and deploy!

Rackspace Private Cloud customers

Coming soon in Rackspace Private Cloud 12.2!
Speak with your account manager for more details.

Anyone on Earth

Use it with your existing Ansible playbooks!
The role works well in OpenStack and non-OpenStack environments (see the docs).

Photo credit: fvanrenterghem (Flickr)

The road ahead:

Support for Ubuntu 16.04 and CentOS 7

Rebase using the new STIG guidelines for RHEL 7

Improved reporting and metrics

Identify configuration security issues within OpenStack services

Want to get involved?
Found a bug?
Have a new idea?

Design Summit:
Join the
OpenStack-Ansible developers
this Thursday/Friday in Austin!

IRC:
#openstack-ansible

Mailing list:
openstack-dev (tag with [openstack-ansible][security])

Links:

Documentation: http://docs.openstack.org/developer/openstack-ansible-security/

Source code: https://github.com/openstack/openstack-ansible-security

COME TO THE

RACKSPACE CANTINA

RELAX | RECHARGE | REFRESH

AT **2ND** AND **TRINITY**

(Right across the street from the Austin Convention Center)

See why it's a **NEW DAWN** for **OPENSTACK** with our **99.99% API UPTIME GUARANTEE.**

#OPENSTACK

rackspace

Thank you!

Major Hayden

major.hayden@rackspace.com

@majorhayden