

# PCI Compliance in the Cloud: A working example

John Knoll

[jpknoll@ucdavis.edu](mailto:jpknoll@ucdavis.edu)

<https://github.com/jpknoll>

Scott Kirkland

[srkirland@ucdavis.edu](mailto:srkirland@ucdavis.edu)

<https://github.com/srkirland>

Adam Getchell

[acgetchell@ucdavis.edu](mailto:acgetchell@ucdavis.edu)

<https://github.com/acgetchell>

UC Computing Systems Conference  
July 10-12 2016  
University of California Santa Cruz

# Goal: Give to UC Davis

- Hired for Centralized Gift Processing
- UC PCI Audit Starts
- Priority Changes: Compliant Website that can take Credit Cards

# Why a complete redesign?

- Replace an onsite Windows Server 2003
  - Oracle Forms Driven
  - ~~Difficult~~ Impossible to bring into compliance
- Switch credit card processors
  - TouchNet to CyberSource
- Modernize look and feel
  - Professional mockups & design
- Be ready before the on site audit (less one year)
  - Agile or Bust!

# Investigate Payment Processors

- TouchNet
- PayPal
- Stripe
- CyberSource / Authorize.Net

Please enter your credit card information

Total:

\$20.00

\* Indicates required information

\* Credit Card Type:

Select a Credit Card Type ▾

\* Account Number:

\* Expiration Date:

07 ▾ 2016 ▾

\* Security Code: ([View example](#))

\* Name on Card:

### Billing Address of Credit Card

\* Street Address 1:

Street Address 2:

\* City:

\* State:

California ▾

\* ZIP Code:

\* Country:

United States ▾

\* Email:

Day Phone:

Night Phone:

Mobile Phone:



[Continue](#)

[Cancel this payment transaction.](#)

# UC Davis Annual Fund

You're donating \$100 to UC Davis Annual Fund .

✓  
Your gift

✓  
About You

⊙  
Payment info

## Finalize your gift!

Enter your payment information 



Name:

John Knoll

Card Number:

4111 1111 1111 1111

Expiration Date:

12 / 34

CVC:

123



Here's what we have so far

John Knoll is making a One Time \$100 donation to UC Davis Annual Fund .

### YOUR DONATION SUPPORTS

UC Davis Annual Fund

Every gift to the UC Davis Annual Fund makes a difference

### CONTACT INFO

Annual and Special Gifts Program

[Annualfund@ucdavis.edu](mailto:Annualfund@ucdavis.edu)

(530) 754-1100 (Phone)

### CATEGORIES

- [annual](#)
- [Innovation](#)
- [leadership](#)
- [students](#)
- [scholarship](#)

### FUND PURPOSE

Unrestricted

### FUND TYPE

CURRENT

# Give to UC Davis

- Demo

# What is PCI?

- Set of standards designed to make payment card processing security the responsibility of all parties involved.
  - Merchant -> Processor -> Bank
- Contractually Enforceable via Bank's Merchant Account
  - Fines, Fee, or Account Termination
- Applies to anyone that accepts credit card payments, even if you don't store cc details.



Goal	Requirement
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Protect all systems against malware and regularly update antivirus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Identify and authenticate access to system components</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

# Meeting Compliance

- The Entire PCI Data Security Standard (DSS) applies to all levels and all environment types.
- Merchant Level (based on business size) Determines how you prove compliance:
  - Annual Self Assessment Questionnaire ("SAQ")
  - Annual Report on Compliances ("ROC") by Qualified Security Assessor ("QSA")

# Merchant Levels

Merchant Level	Description
1	Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.

SAQ Type	Description	# Q's
A	Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage	14
A-EP	E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage	139
B	Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage	41
B-IP	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage	83
C	Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage	139
C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage	73
D-MER	All other SAQ-eligible merchants	326
D-SP	SAQ-eligible service providers	347
P2PE	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	35

SAQ Type	Description	# Q's
<b>A</b>	<b>Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage</b>	<b>14</b>
<b>A-EP</b>	<b>E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage</b>	<b>139</b>
B	Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage	41
B-IP	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage	83
C	Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage	139
C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage	73
<b>D-MER</b>	<b>All other SAQ-eligible merchants</b>	<b>326</b>
D-SP	SAQ-eligible service providers	347
P2PE	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	35



# Choosing a platform

- Build Server + Continuous Integration
- Web Servers
- Load Balancer / Traffic Management
- Database
- Storage
- Logging
- Email
- Search Provider
- Web Jobs

# Choosing a platform

- Build Server + Continuous Integration: [AppVeyor](#)
- Web Servers: [Azure Web Sites](#)
- Load Balancer / Traffic Management: [Azure](#)
- Database: [Azure SQL Database](#)
- Storage: [Azure Storage](#)
- Logging: [Stackify](#)
- Email: [SparkPost](#)
- Search Provider: [Elastic Search via Compose.io](#)
- Web Jobs: [Azure Web Jobs](#)



# Why the Cloud?

- Better
- Faster
- Cheaper
- Stronger



# Better - Agile Method

Contributors

Traffic

Commits

Code frequency

Punch card

Network

Members

Jun 1, 2014 – Dec 24, 2014

Contributions to master, excluding merge commits

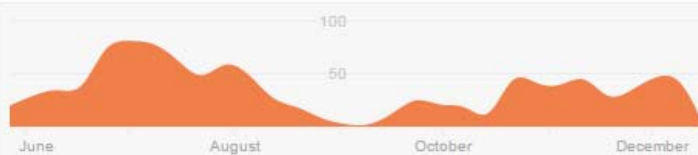
Contributions: Commits ▾



jpknoll

1,056 commits / 278,923 ++ / 267,926 --

#1



cydoval

677 commits / 117,773 ++ / 98,177 --

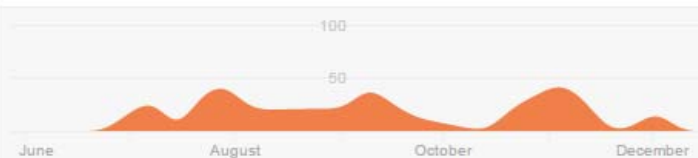
#2



jSylvestre

479 commits / 80,965 ++ / 9,916 --

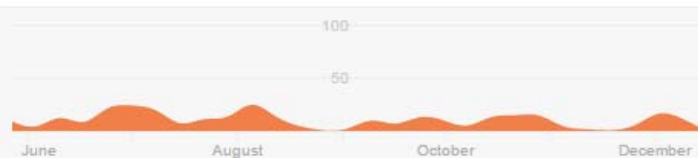
#3



srkirkland

308 commits / 243,229 ++ / 17,376 --

#4





CGP-TESTING ☆ Private

Ready for test-STAGE

Pledge is requiring a coupon scan  
3 1 ZM

Not Receiving Expected Notification Given Role in STAGE  
3 KB

Splitting a gift as a modification after the gift has been processed and batch processing is complete (Gift is in 'Financial Review' status).  
6

Batch images in Advance do not show donor update info  
7 1 ZM

Update title for 'Shrem Museum of Art Unit GREAT User'  
3

Special Instructions  
5 ZM

LGS Not Getting Notifications when Gifts are Moved into Modification Required  
4 KB

Missing GREAT ID/Receipt Number/Other Identifying

Add a card...

Ready for Production

GREAT PROD Deployment 6/27  
3 0/12

GREAT PROD Deployment 6/14  
2 0/10

GREAT PROD Deployment 6/2  
0/12

GREAT PROD - Deployment 5/3  
0/8

GREAT PROD Deployment 4/12  
1/9

GREAT PROD Deployment 3/29  
0/6

HIGH: Production release 3/22/16  
2 1/13

Payment Information

Total Amount Received  
\$ 100

Date Received  
06/21/2016

What form of payment was used?  
Check/Cash

Send tender by  
Net Sent

Check number (or enter "CASH")  
# Check number or "CASH"

Approval Code

Check Number Field Can Be Required  
4 1 ZM

Add a card...

Production Items that Need Testing

CARDS THAT NEED PROD TESTING WILL GO HERE.  
0/2

Create Bulk Entry Button - no indication of created entry when clicked.  
1 KB

READY FOR PROD-Update functionality to include GREAT-Multiples AQ2 LB type.  
10 1



GREAT New Pledge Amount Issue  
11 1



Multiple Roles Fail on Financial Details Link for Completed Gifts  
7 8

Add a card...

AIS-Internal Testing Items

NEW! Advance Stewardship Report in STAGE  
1

GREAT- Proceeds Check (Check only)  
6

HIGH: Testing Manual Check Processing-Using Coupon Only  
3

HIGH: Foundation Endowments & Quasi  
18 2

HIGH: Testing Rejected Check Processing-Using Coupon Only  
1

MEDIUM: Saving an excel and pdf export under a different name in GREAT loses the file type.  
4

Giving: Speed improvements on list pages (Test as part testing process)  
1

Add a card...

AIS-Internal Items-Additional Action

NEW: Ability to cha type while an entry  
3

PASS-READY TO F PHASE 2-GREAT C when/how to proce  
8

Double reconcile is fix) (Jan 28 an acci double reconcile oc he will look into cod prevent this in futur need a procedure i meantime?  
5 1

CHECKLIST  
0/5

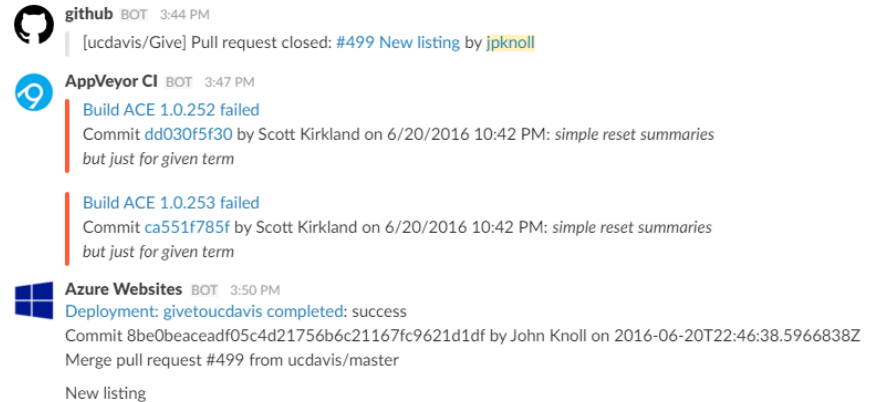
HIGH: Add 'Manual the 'All Gifts' and 'A status filter options. to the 'All Financial option.  
10

MEDIUM: More use experience for the ' Reviewer roles.  
3

Add a card...

# Faster - Deployment Strategies

- Test Instances
  - Staging Slots
- Continuous Integration
  - Automated build + test (Appveyor, OctoDeploy)
- Deployment Notification
  - Slack/Chat, Email, Ticketing System



The screenshot displays a chat log with three distinct messages from different bots:

- github BOT 3:44 PM**: [ucdavis/Give] Pull request closed: #499 New listing by [jpknoll](#)
- AppVeyor CI BOT 3:47 PM**:
  - Build ACE 1.0.252 failed  
Commit [dd030f5f30](#) by Scott Kirkland on 6/20/2016 10:42 PM: *simple reset summaries but just for given term*
  - Build ACE 1.0.253 failed  
Commit [ca551f785f](#) by Scott Kirkland on 6/20/2016 10:42 PM: *simple reset summaries but just for given term*
- Azure Websites BOT 3:50 PM**:
  - Deployment: [givetoucDavis](#) completed: success
  - Commit [8be0beaceadf05c4d21756b6c21167fc9621d1df](#) by John Knoll on 2016-06-20T22:46:38.5966838Z
  - Merge pull request #499 from ucdavis/master
  - New listing

# Cheaper - Costs and Scaling

- Build Server + CI: \$40
- Web Server: \$40 x 2
- Load Balancer / Traffic Management: Free
- Database: \$15 x 2
- Storage: < \$1
- Email: \$15
- Logging + APM: \$40 (10GB / month)
- Search Provider: \$50
- Web Jobs: Free
  
- Total: \$255.99 / month

The screenshot shows the 'Scale setting' interface for a 'ProductionPool'. At the top, there are 'Save' and 'Discard' buttons. Below is a line graph showing the number of instances over time from July 4 to July 10. The y-axis is labeled 'INSTANCES' and ranges from 0 to 0.6. A large '1' is displayed below the graph, indicating the current number of instances. The 'Scale by' dropdown is set to 'CPU Percentage'. The 'Description' reads: 'Automatically scale up or down based on CPU Percentage. Choose an average value you want to target.' The 'Instances' slider is set to 1. The 'Target range' is set from 60 to 80. At the bottom, there are notification settings: 'Email Administrator and CoAdministrators' is unchecked, 'Additional email(s)' is empty, and 'Webhook' is checked with an empty URL field. A link to 'Learn more about configuring webhooks for autoscale notifications' is provided.

# Stronger - Reduced PCI Scope

- Shared Responsibility Model
- Decreased complexity
- Less control over security modes (This is a good thing!)

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer
Client & end-point protection	Cloud Customer	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider
Identity & access management	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Customer / Cloud Provider
Application level controls	Cloud Customer	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider
Network controls	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Host infrastructure	Cloud Customer	Cloud Customer / Cloud Provider	Cloud Provider	Cloud Provider
Physical security	Cloud Customer	Cloud Provider	Cloud Provider	Cloud Provider

Legend: ■ Cloud Customer ■ Cloud Provider

From Azure PCI DSS Responsibility Matrix 2016

# Physical Security

- No access;  
Fully managed



# Patch Management

- Infrastructure Patching & Configuration
  - OS, Framework, WebServer
  - Managed by Azure, secure by default
- Application Development
  - Secure SDLC
- 3<sup>rd</sup> Party Libraries
  - Package management



# Network & Firewalls

- Partial Management by Azure
  - Single Endpoint
- DB Servers have firewall rules too!
- Business Justifications

Firewall settings  
[server name] (SQL server)

Save Discard Add client IP

Connections from the IPs specified below provides access to all the databases in [server name].

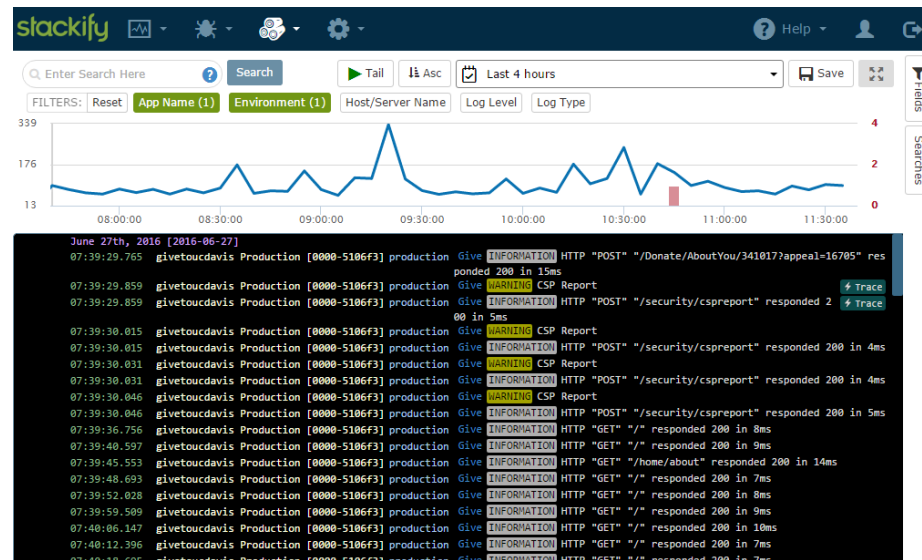
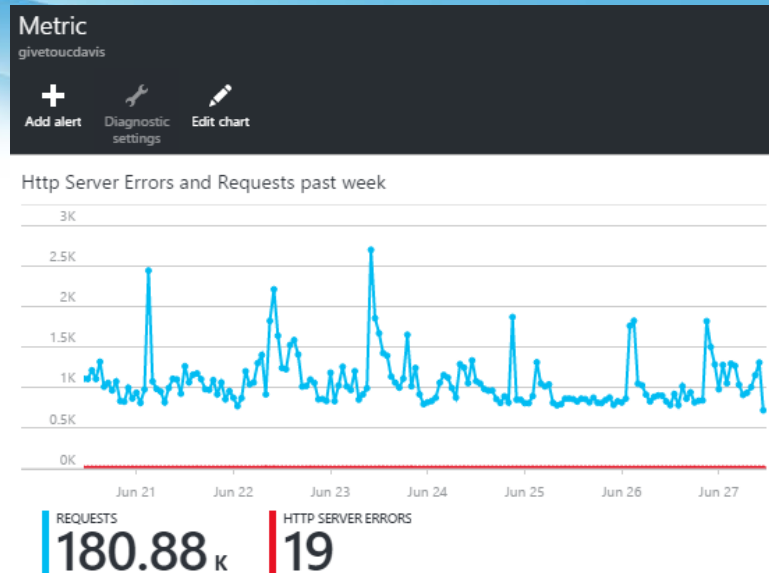
Allow access to Azure services  ON  OFF

Client IP address

RULE NAME	START IP	END IP	
<input type="text"/>	<input type="text"/>	<input type="text"/>	...
CAESDO	<input type="text"/>	<input type="text"/>	...
CAESDO2	<input type="text"/>	<input type="text"/>	...
DEVAR	<input type="text"/>	<input type="text"/>	...

# Logging

- Management by Azure
  - OS, IIS, ASP.Net
- Application Level Logging
  - Stackify
- Logs are useless if you don't watch them
  - Demo



# Account Management

- Enforced by Microsoft Live + Internal Policies



## settings

SUBSCRIPTIONS MANAGEMENT CERTIFICATES ADMINISTRATORS AFFINITY GROUPS USAGE REMOTEAPP

NAME	SUBSCRIPTION	SUBSCRIPTION ID	ROLE
<input type="text"/>	UC Davis DEVAR	<input type="text"/>	Service administrator
<input type="text"/>	UC Davis DEVAR	<input type="text"/>	Co-administrator
<input type="text"/>	UC Davis DEVAR	<input type="text"/>	Co-administrator
<input type="text"/>	UC Davis DEVAR		

## Microsoft account

### Help us protect your account

Because you've turned on two-step verification, we need to verify your identity. Enter the code generated by your authenticator app.

I sign in frequently on this device. Don't ask me for a code.

Submit

Cancel

If you can't use an app right now, [get a code a different way.](#)

## Two-step verification

Your account is protected by two-step verification.

[Turn off two-step verification](#)

Goal	Requirement
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> <li>5. Protect all systems against malware and regularly update antivirus software or programs</li> <li>6. Develop and maintain secure systems and applications</li> </ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li>8. Identify and authenticate access to system components</li> <li>9. Restrict physical access to cardholder data</li> </ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security for all personnel</li> </ol>

Goal	Requirement
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect cardholder data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>
Protect Cardholder Data	<ol style="list-style-type: none"> <li>3. Protect stored cardholder data</li> <li>4. Encrypt transmission of cardholder data across open, public networks</li> </ol>
<b>Maintain a Vulnerability Management Program</b>	<ol style="list-style-type: none"> <li>5. Protect all systems against malware and regularly update antivirus software or programs</li> <li><b>6. Develop and maintain secure systems and applications</b></li> </ol>
<b>Implement Strong Access Control Measures</b>	<ol style="list-style-type: none"> <li>7. Restrict access to cardholder data by business need to know</li> <li><b>8. Identify and authenticate access to system components</b></li> <li>9. Restrict physical access to cardholder data</li> </ol>
<b>Regularly Monitor and Test Networks</b>	<ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li><b>11. Regularly test security systems and processes</b></li> </ol>
<b>Maintain an Information Security Policy</b>	<b>12. Maintain a policy that addresses information security for all personnel</b>

# Difficulties – SSL and Early TLS

## How can we improve Azure Web Apps (formerly Websites)?

– Web Apps (formerly Websites)

274

votes

Vote

### Disable Insecure Ciphers In Azure Websites

Either through a configuration/scale option, or just blanket by default, I want to be able to disable RC4 ciphers (and any other insecure cipher suites) in Azure Websites so I can get an A rating (or better) from the Qualys SSL Labs SSL Server Test (<https://www.ssllabs.com/ssltest/analyze.html>).

At present, the only way to do this is not use Azure Websites and host your own VM where you can configure the registry to disable such ciphers.

 **Martin Costello** shared this idea · February 13, 2015 · [Flag idea as inappropriate...](#)



**COMPLETED** · **Cory Fowler** responded · October 01, 2015

Marking this item as completed. RC4 was disabled across the service by the end of August.

[Show previous admin responses \(3\)](#)

## RC4 Support (2015)

4

votes

Vote

### Either sun set TLS 1.0 or give users the means to disable it

We chose Azure App Services to host a new web application which was scheduled to go live by the end of March, 2016. Incredibly, we are now finding that TLS 1.0 cannot be disabled on App Services. Because of that, we cannot pass a PCI DSS 3.1 scan. We've looked through all of the posts and replies on MS forums related to this, but there is no answer to the specific question we have. We understand that there are alternative hosting solutions like ASE and Web Roles where MS has the means to disable TLS 1.0. Both of these represent additional time and effort to setup and deploy our QA and production sites, and both represent additional compute costs for resources that we definitely don't need (i.e., we have no worker processes and would prefer to not pay for worker instances). We also understand that PCI is requiring new applications to be DSS 3.1 compliant even though they have extended the deadline for existing applications to June, 2018.

So, the question is whether Microsoft is planning to give users the ability to disable TLS 1.0 in ordinary (i.e., non-ASE) App Services. Or, will you finally be sun setting TLS 1.0 in ordinary App Services? All of the replies referred to above were extremely vague about what exactly is on the roadmap for App Services. Could we please have a definitive answer whether we will have this ability to disable TLS 1.0 before the June, 2018 deadline? If so, we may be able to prepare a mitigation and migration plan that would grant us an exception to the DSS 3.1 compliance.

For what it's worth, we came to Microsoft because it appeared to be the clear PaaS leader. Please tell us that MS thought this through and has a cost effective PaaS strategy that is consistent with the entire industry regarding secure protocols. If not, then what differentiates Azure VMs from AWS VMs?

 **Anonymous** shared this idea · March 23, 2016 · [Flag idea as inappropriate...](#)

### 1 comment

Add a comment...

Your email address

or sign in with 

Post comment



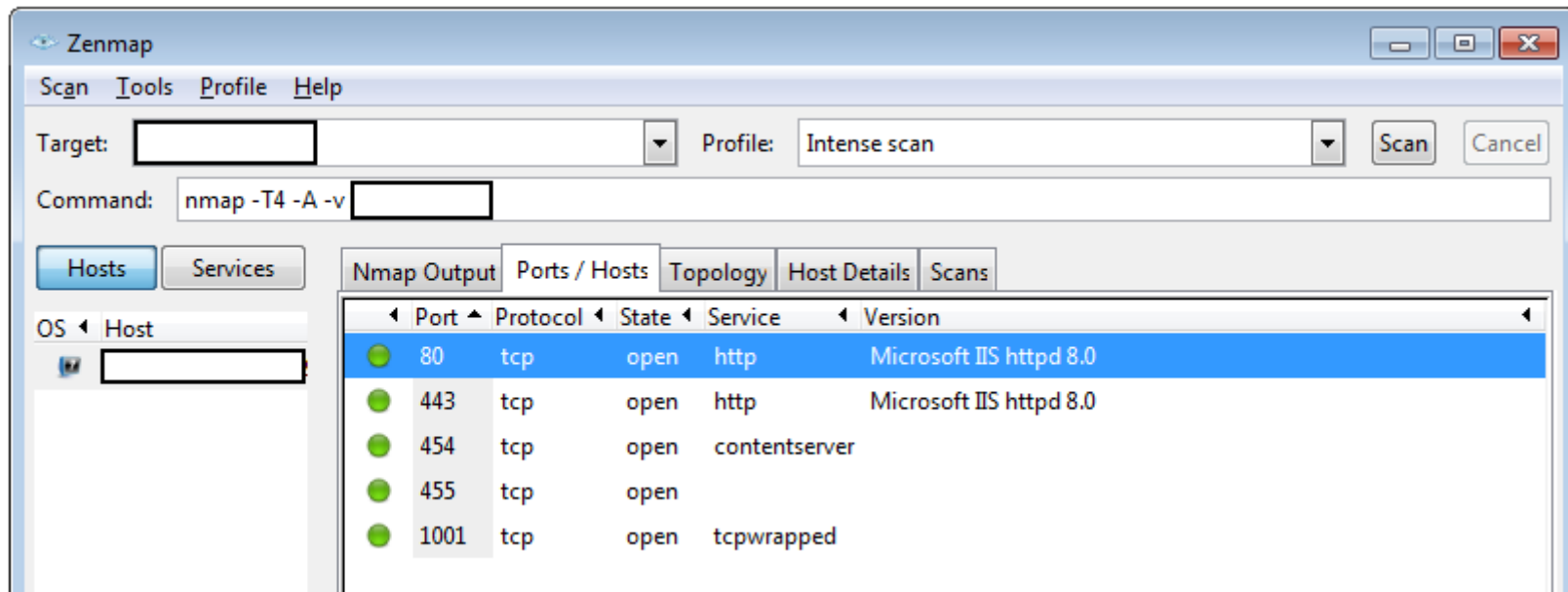
**Cory Fowler** commented · March 23, 2016 16:16 · [Flag as inappropriate](#)

Note that the PCI standards board updated their guidance for PCI v 3.1 and pushed out the date for removing TLS 1.0 to June 2018.

## TLS 1.0 Support (2018)

# Difficulties - Network Scanning

- Uncontrolled Ports & Services
  - 454/455/1001: Internal Web Service Apps



# Difficulties - Penetration Test

- Advanced Notice Required
  - Disruptive to Cloud Platform
- Unknown protective measures, responses, reactions
- Black Box by default



# Difficulties – Understanding the Cloud

- Auditor didn't understand our infrastructure



# Results

- Passed our Audit!
- Started our SAQ-A-EP last week

# Results

- 746 unique funds
- 5000+ gifts, 173 recurring
  - Recurring is a new feature
- \$1,495,055.41 raised
  - 20% increase over previous year

# Reference

- PCI FAQs:
  - <https://www.pcicomplianceguide.org/pci-faqs-2/>
  - <http://www.pkfavantedge.com/it-compliance/pci-dss-and-the-saqs-that-sucks/>
- Microsoft Trust Center
  - <https://www.microsoft.com/en-us/TrustCenter/Compliance/PCI>
  - Azure PCI DSS Responsibility Matrix 2016
- Amazon Web Services (AWS) Clour Security
  - <https://aws.amazon.com/compliance/pci-dss-level-1-faqs/>
- Azure UserVoice
  - <https://feedback.azure.com/forums/169385-web-apps-formerly-websites/suggestions/7091994-disable-insecure-ciphers-in-azure-websites>
  - <https://feedback.azure.com/forums/169385-web-apps-formerly-websites/suggestions/13097865-either-sun-set-tls-1-0-or-give-users-the-means-to>