

# CSC 9

*John Ryan Zelling Analyst*

*Jan 2017*

## Contents

<b>CSC 9.0</b>	<b>1</b>
CSC 9.1 . . . . .	2
CSC 9.2 . . . . .	4
CSC 9.3 . . . . .	6
CSC 9.4 . . . . .	8
CSC 9.5 . . . . .	10
CSC 9.6 . . . . .	12

## CSC 9.0

[1] “Critical Security Control #9: Limitation and Control of Network Ports”

1

---

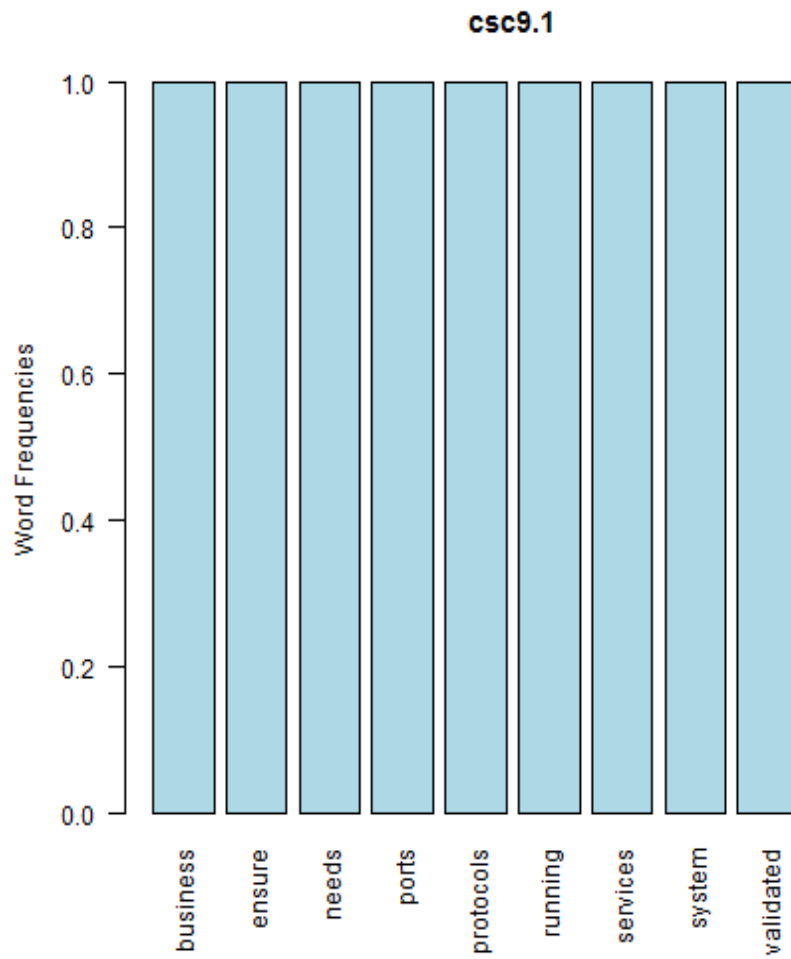
<sup>1</sup>[1] “To further clarify the Creative Commons license related to the CIS Critical Security Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Critical Security Controls, you may not distribute the modified materials. Users of the CIS Critical Security Controls framework are also required to refer to (<http://www.cisecurity.org/critical-controls.cfm>) when referring to the CIS Critical Security Controls in order to ensure that users are employing the most up to date guidance. Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security.”

## CSC 9.1

[1] “business + ensure”

validated  
services  
ports  
needs  
business  
ensure  
protocols  
running  
system

null device 1



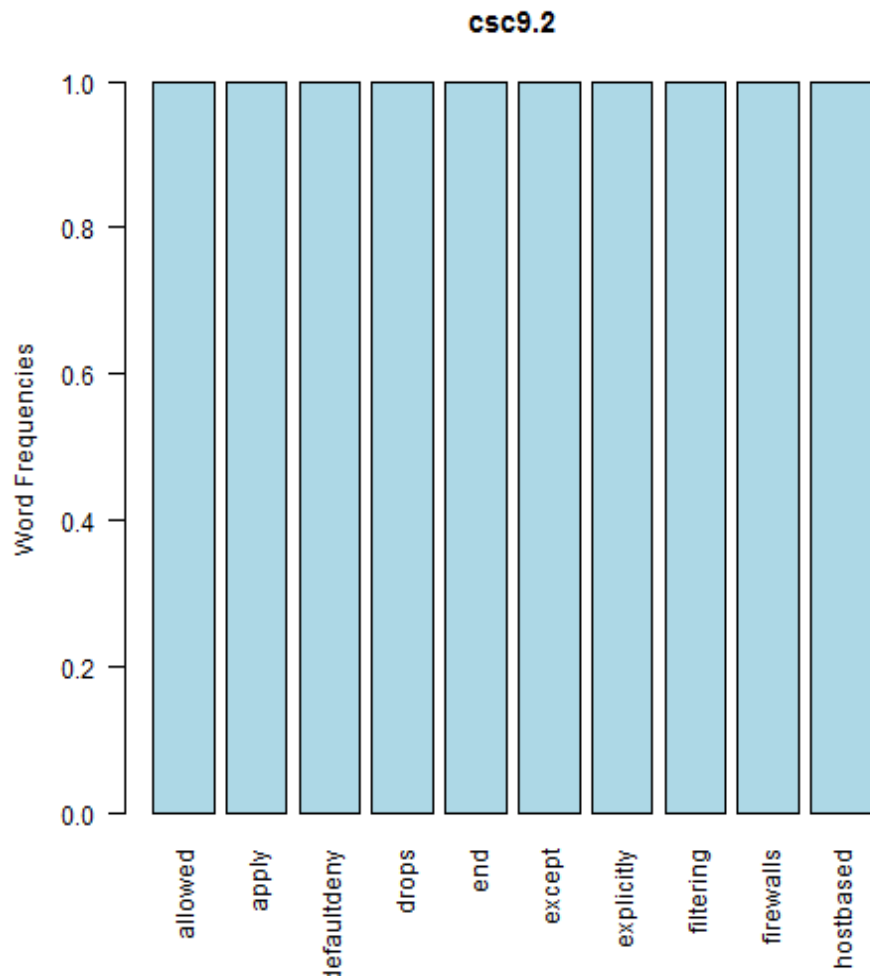
null device 1 [1] “Ensure that only ports, protocols, and services with validated business needs are running on each system.”

## CSC 9.2

[1] “allowed + apply”

le firewalls  
except  
end pool  
apply  
allowed explicitly  
default deny  
drops  
filtering port  
tools  
hostbased

null device 1



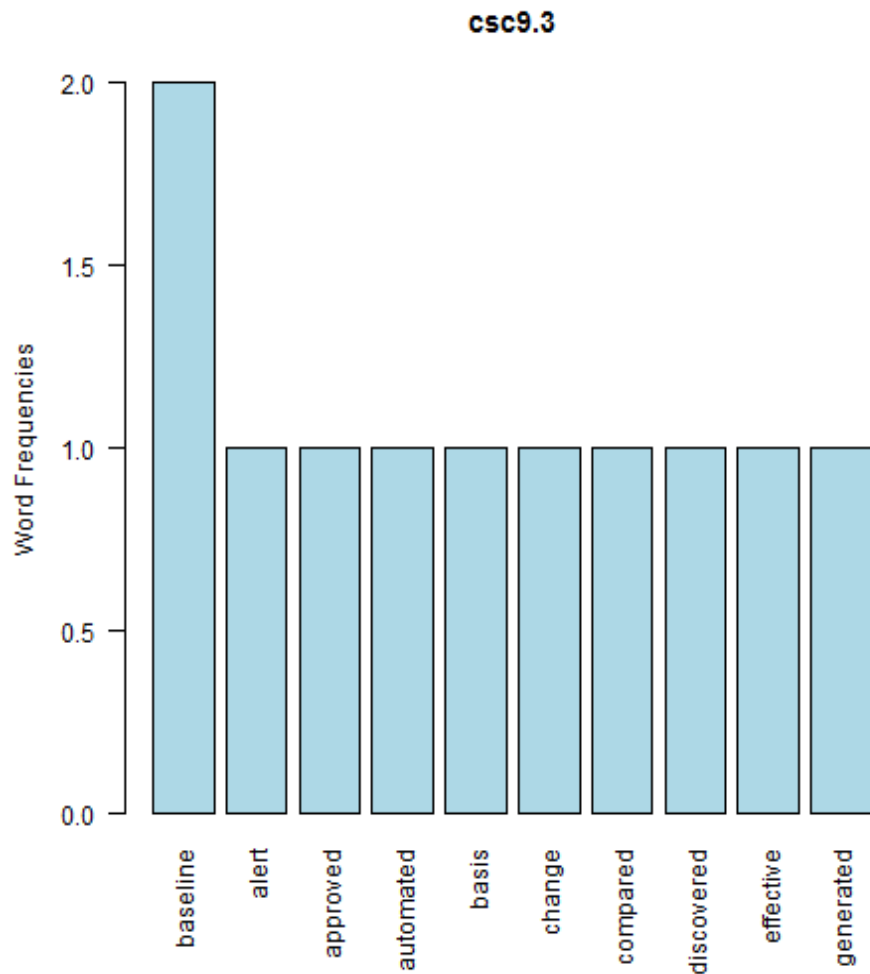
null device 1 [1] “Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.”

## CSC 9.3

[1] “baseline + alert”

A word cloud with the word "baseline" in the center, rendered in a large, bold, dark blue font. Surrounding it are various other words in a magenta color, of varying sizes and orientations. The words include: "organizationâ€™s", "perform", "effective", "approved", "reviewed", "listed", "discovered", "automated", "port", "known", "compared", "basis", "serve", "scan", "regular", "generated", "change", "alert", and "key". The words are arranged in a circular pattern around the central "baseline" word.

null device 1



null device 1 [1] “Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization’s approved baseline is discovered, an alert should be generated and reviewed.”

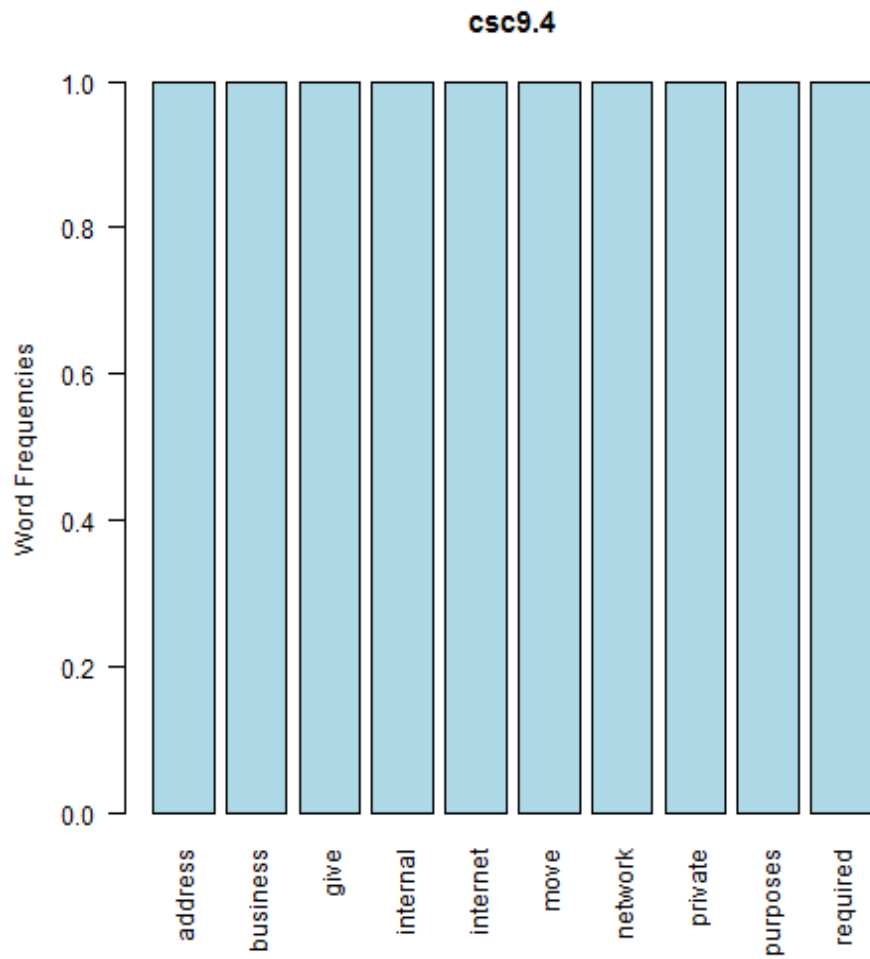
## CSC 9.4

[1] “address + business”

visible required  
private  
vian server  
move internal  
address network  
interne  
give  
business  
purposes verify

null device 1





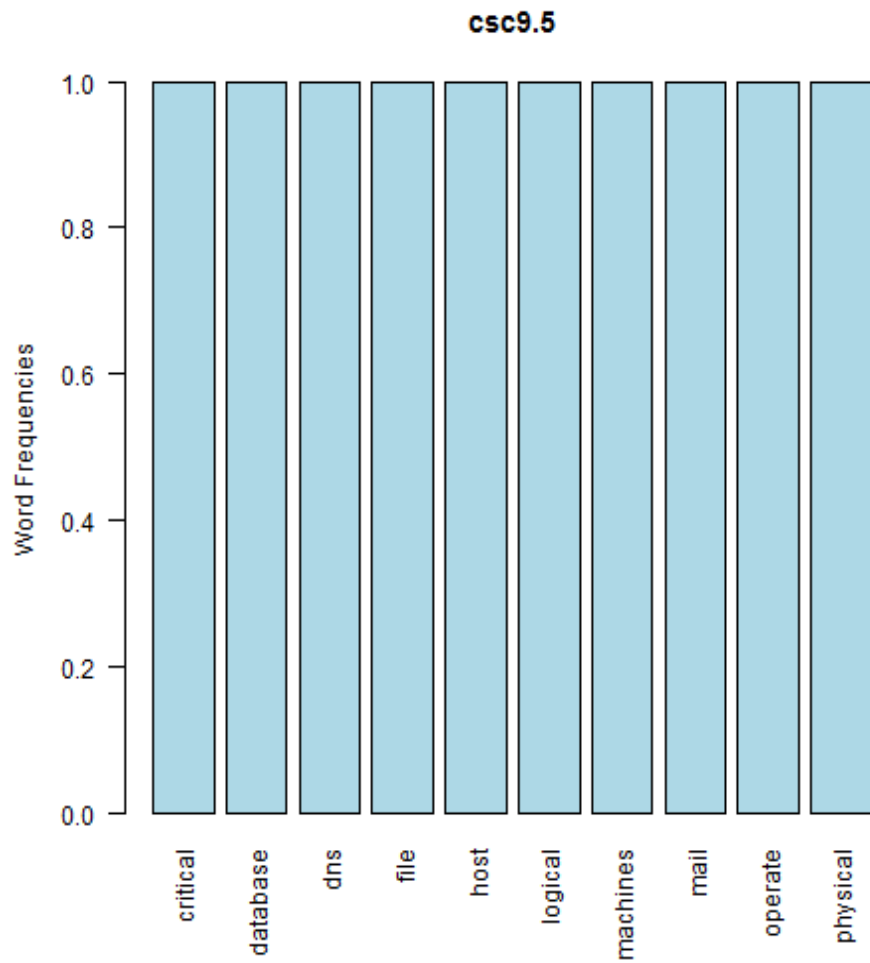
null device 1 [1] “Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.”

## CSC 9.5

[1] “critical + database”

machines  
web  
separate  
serve  
physical  
logical  
database  
critical  
file  
dns  
host  
mail  
operate

null device 1



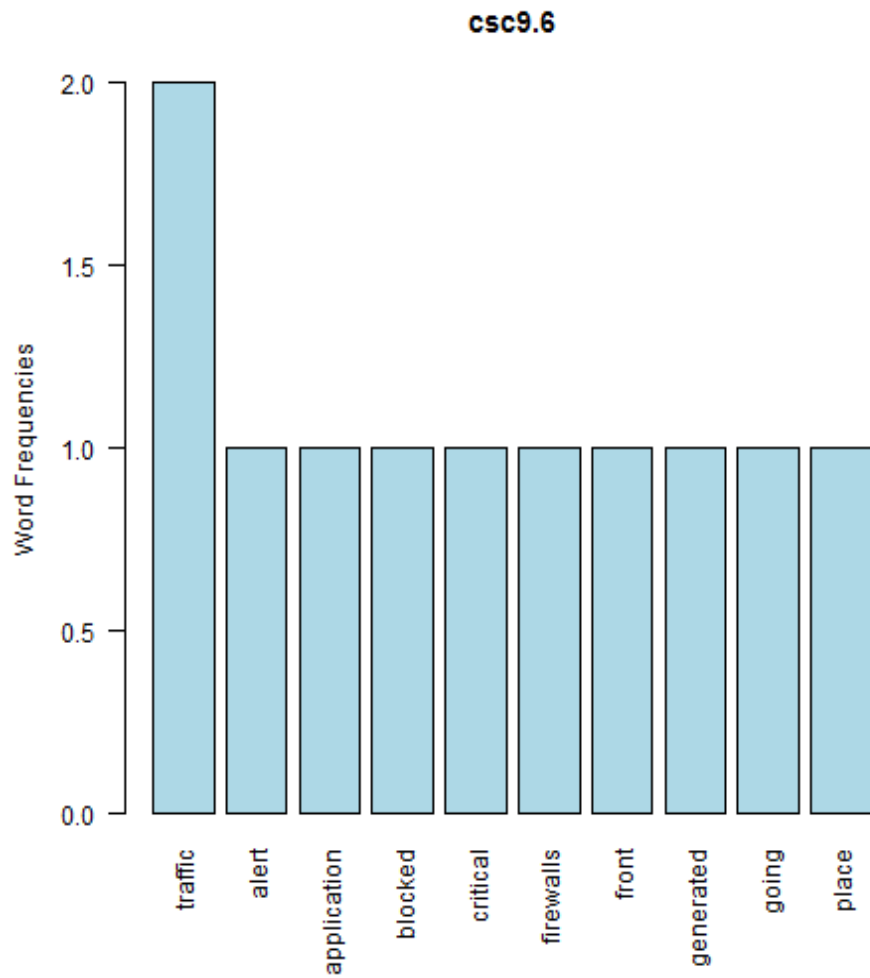
null device 1 [1] “Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.”

## CSC 9.6

[1] “traffic + alert”



null device 1



null device 1 [1] “Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.”