CSC 5

John Ryan Zelling Analyst

Jan 2017

Contents

CSC 5.0

[1] "Critical Security Control #5: Controlled Use of Administrative Privileges"

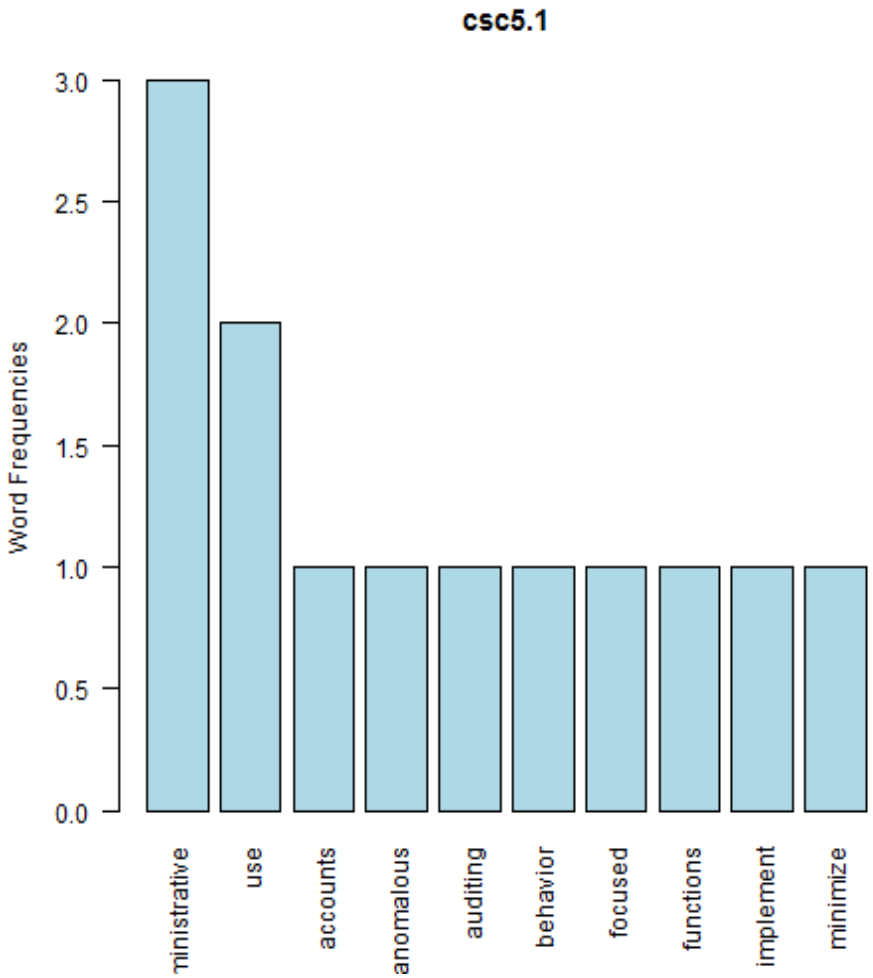
[1]

[1] [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. Â 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 ControlsÂ in order to ensure that users are employing the most up to date guidance. Â Commercial use of the CIS Critical Security Controls is subject to the prior approval of The Center for Internet Security."

CSC 5.1

[1] “administrative + use”

null device 1

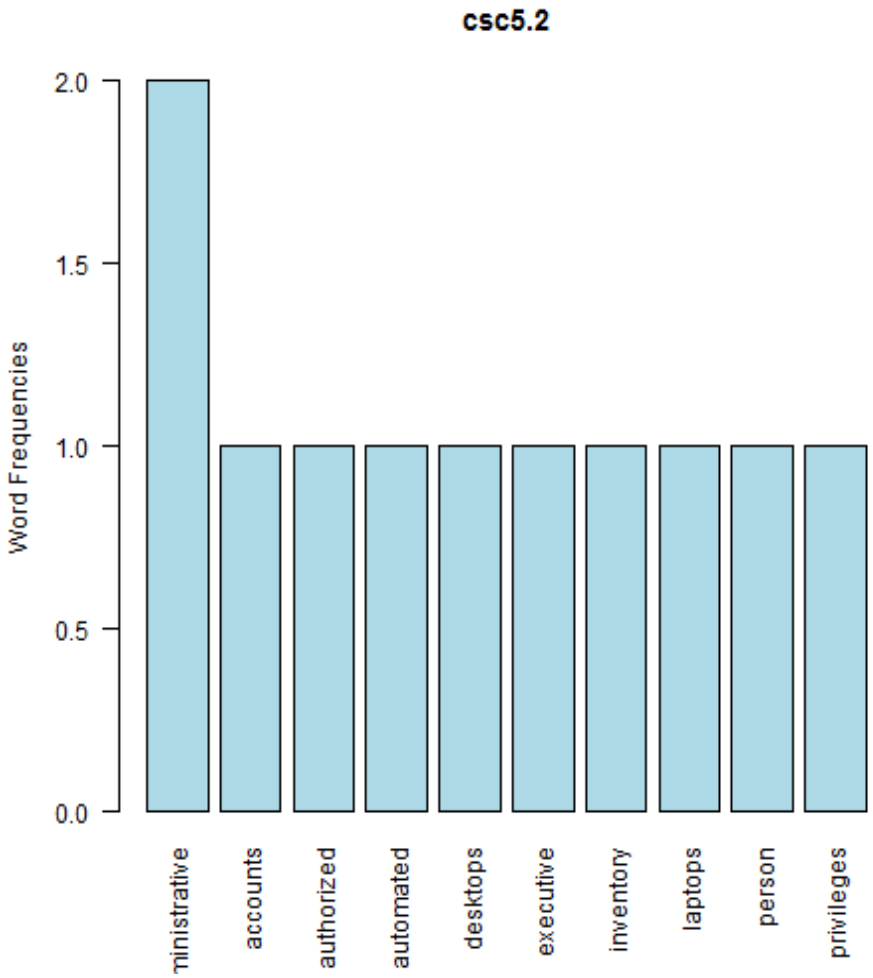


null device 1 [1] “Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.”

CSC 5.2

[1] “administrative + accounts”

null device 1

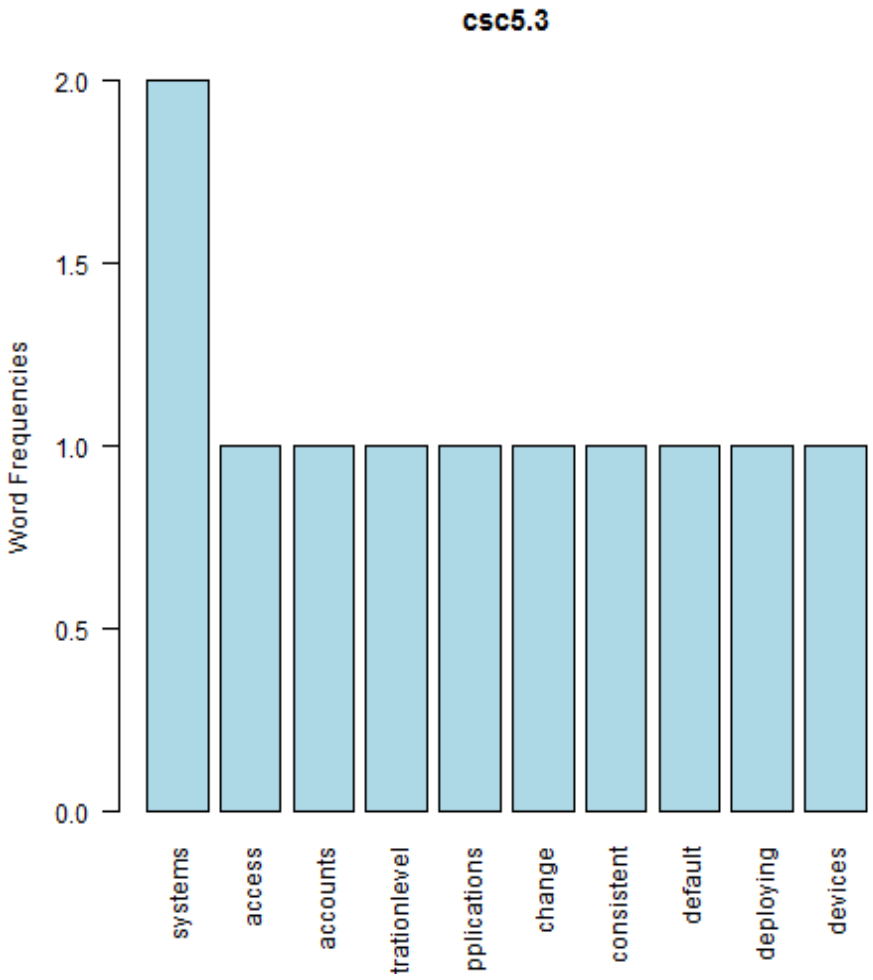


null device 1 [1] “Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.”

CSC 5.3

[1] “systems + access”

null device 1

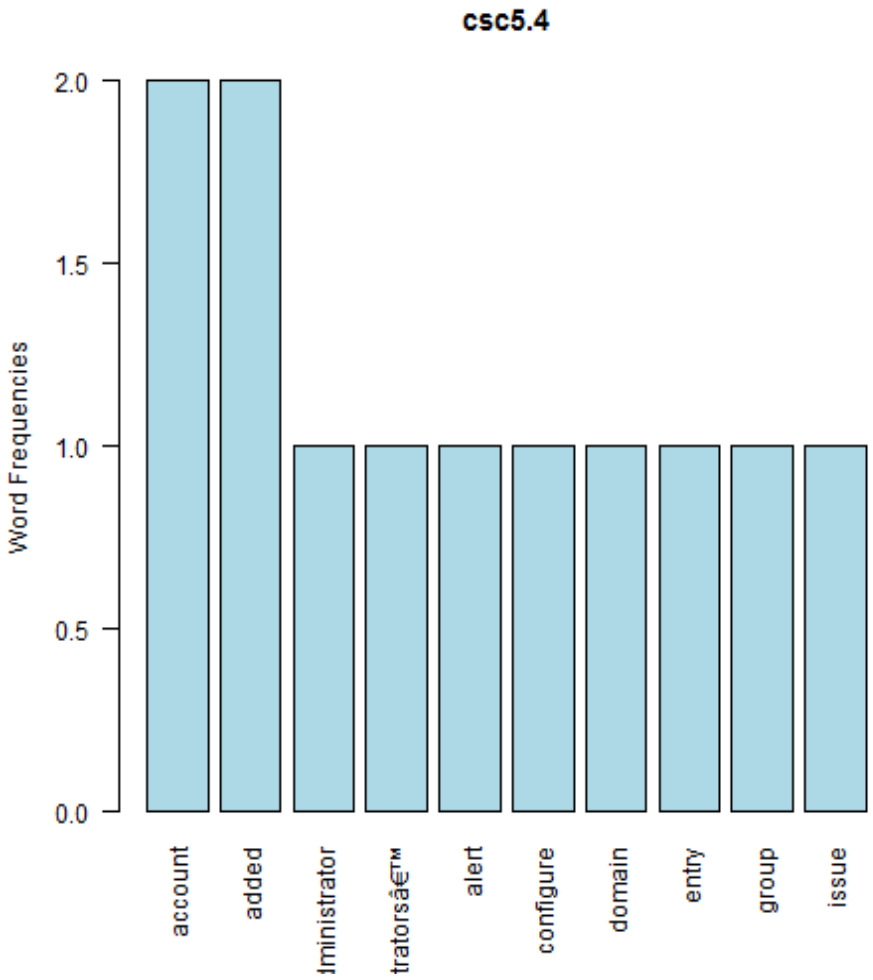


null device 1 [1] “Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.”

CSC 5.4

[1] “account + added”

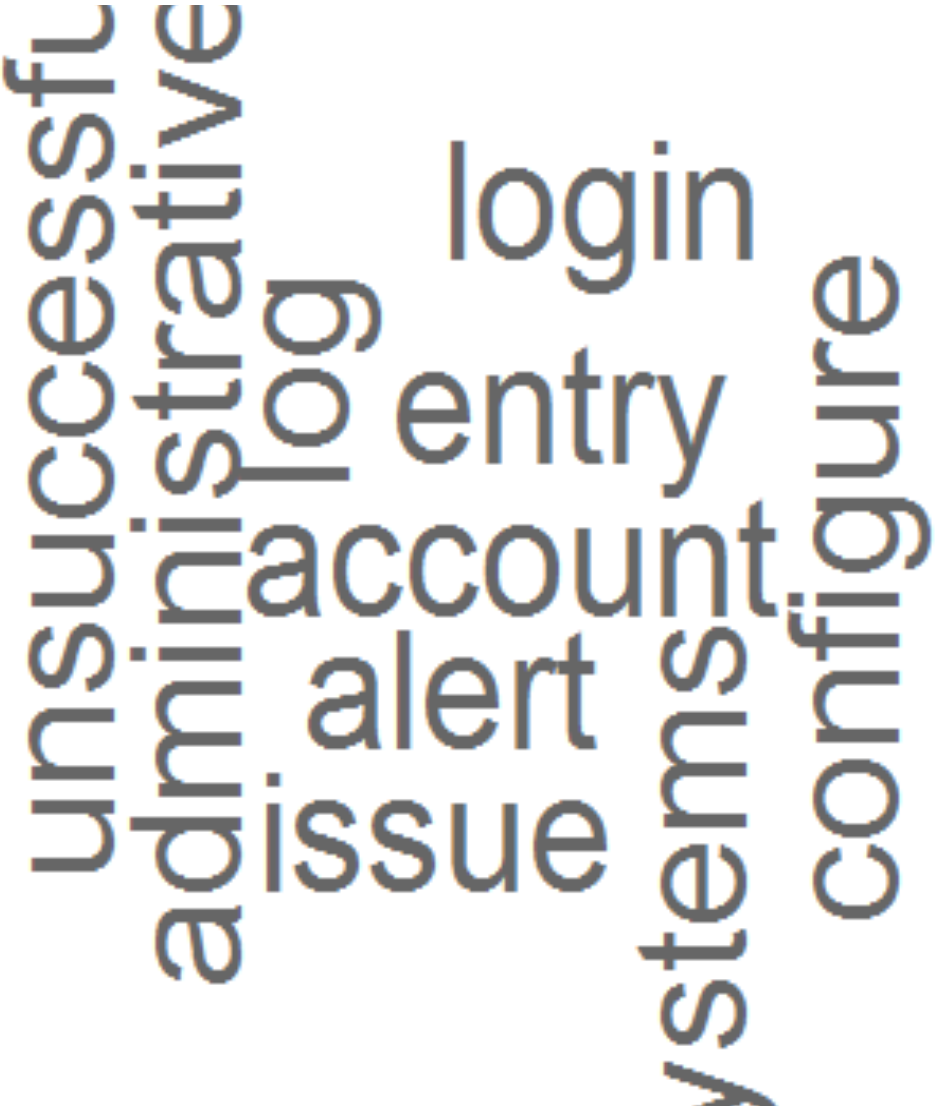
null device 1



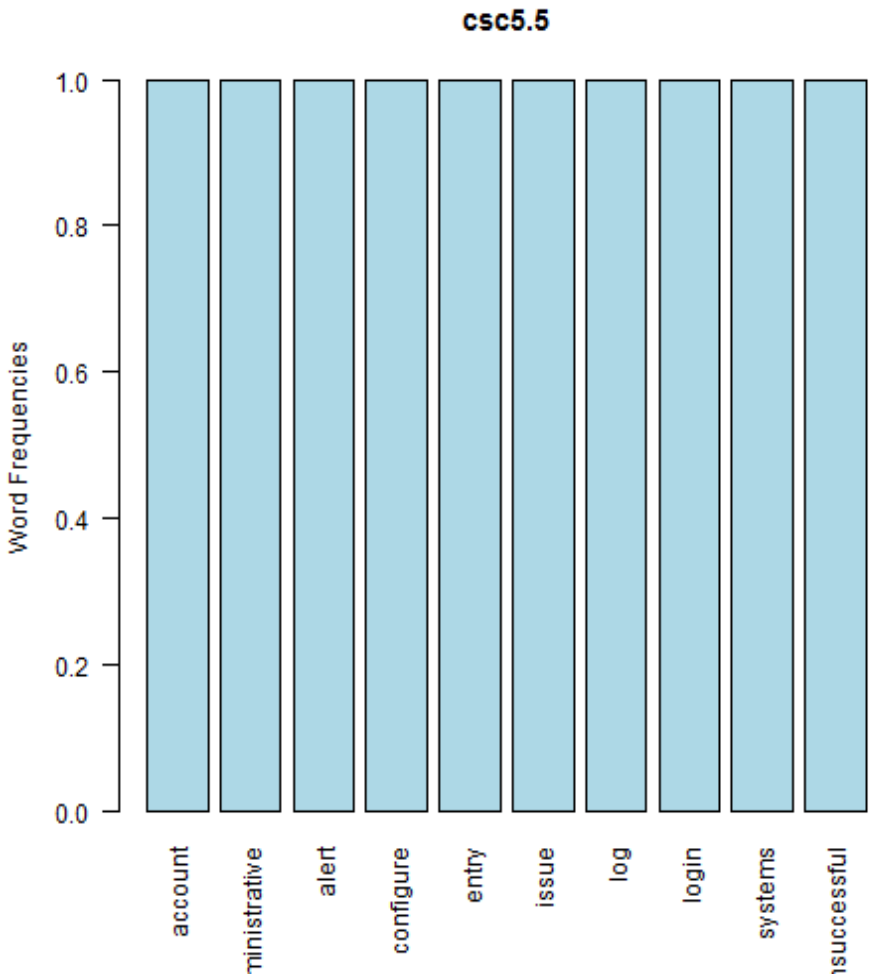
null device 1 [1] “Configure systems to issue a log entry and alert when an account is added to or removed from a domain administratorsâ group, or when a new local administrator account is added on a system.”

CSC 5.5

[1] “account + administrative”



null device 1

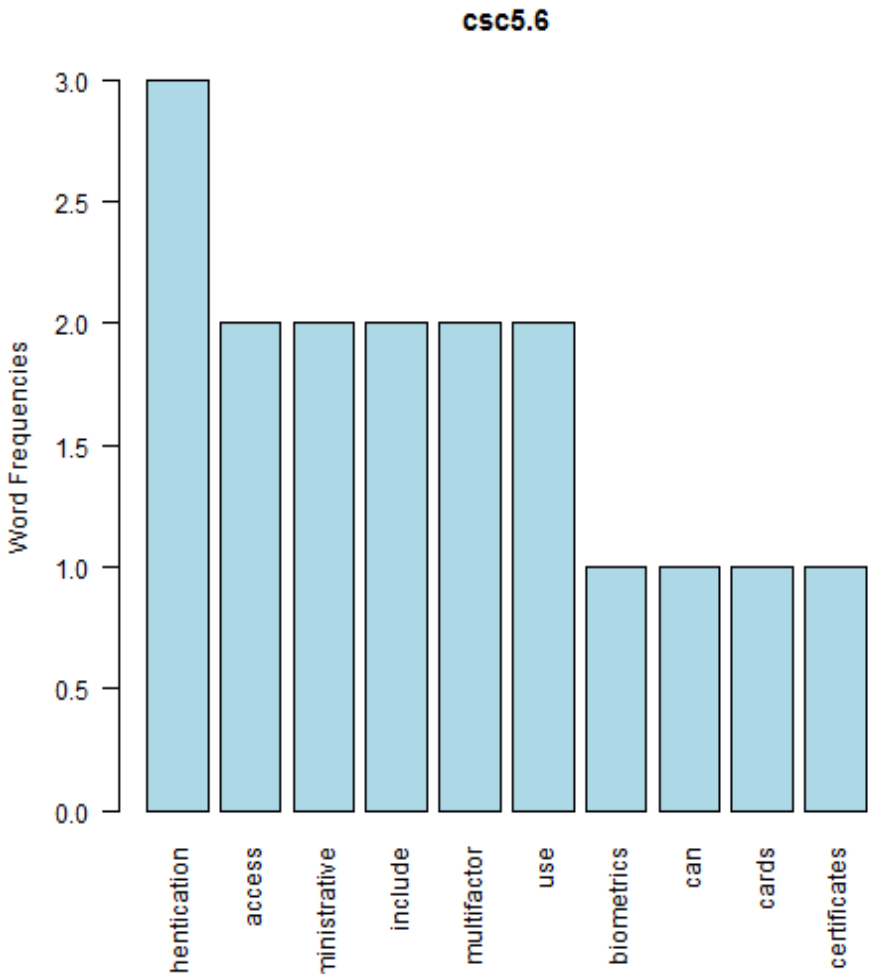


null device 1 [1] “Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.”

CSC 5.6

[1] “authentication + access”

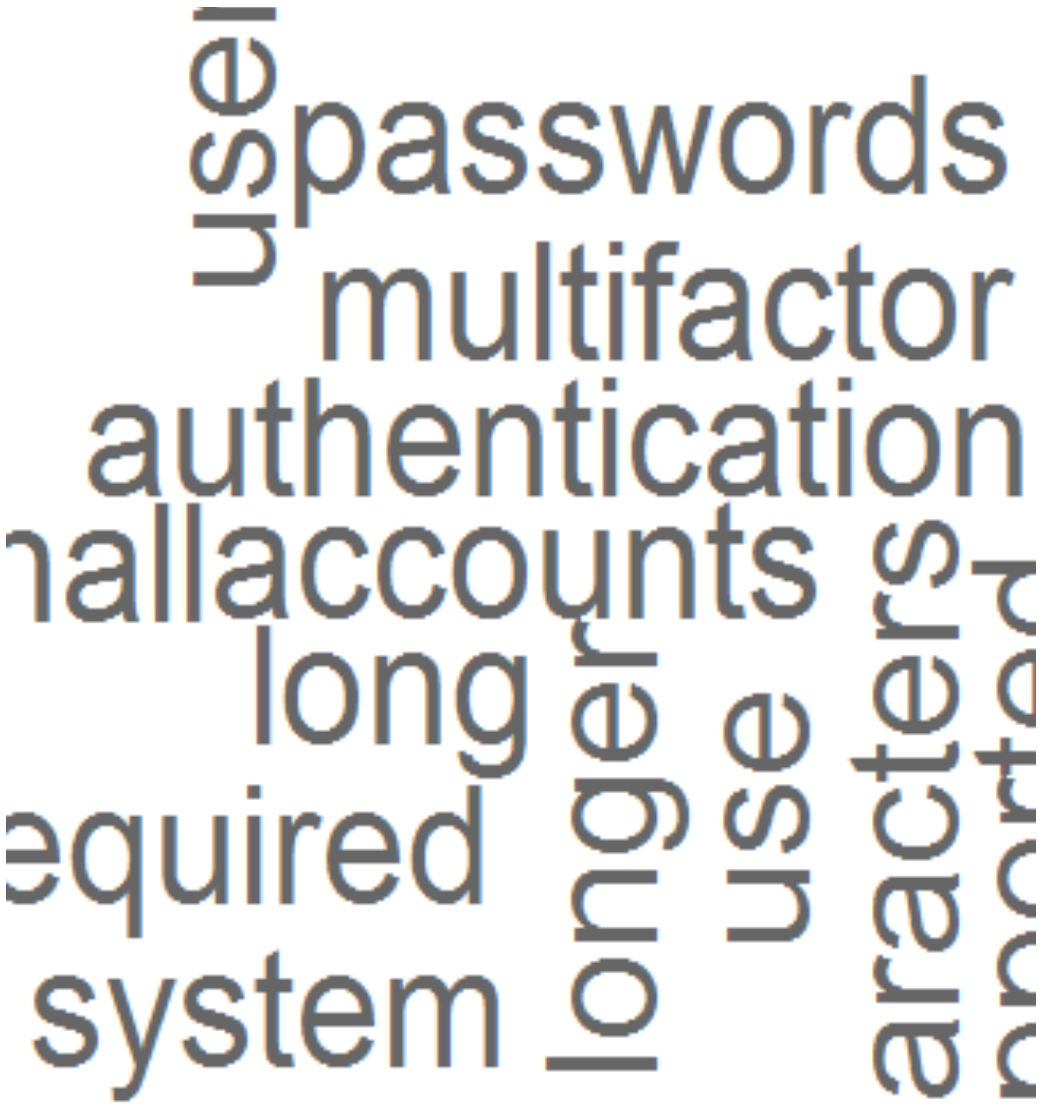
null device 1



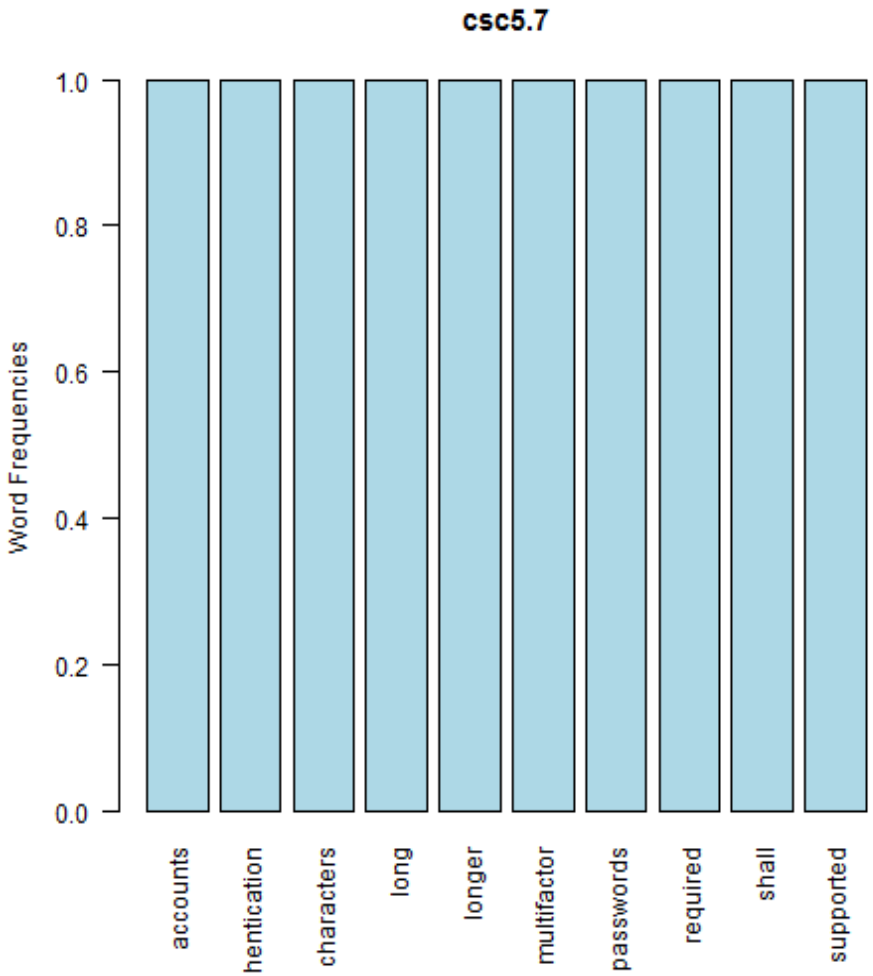
null device 1 [1] "Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods."

CSC 5.7

[1] “accounts + authentication”



null device 1

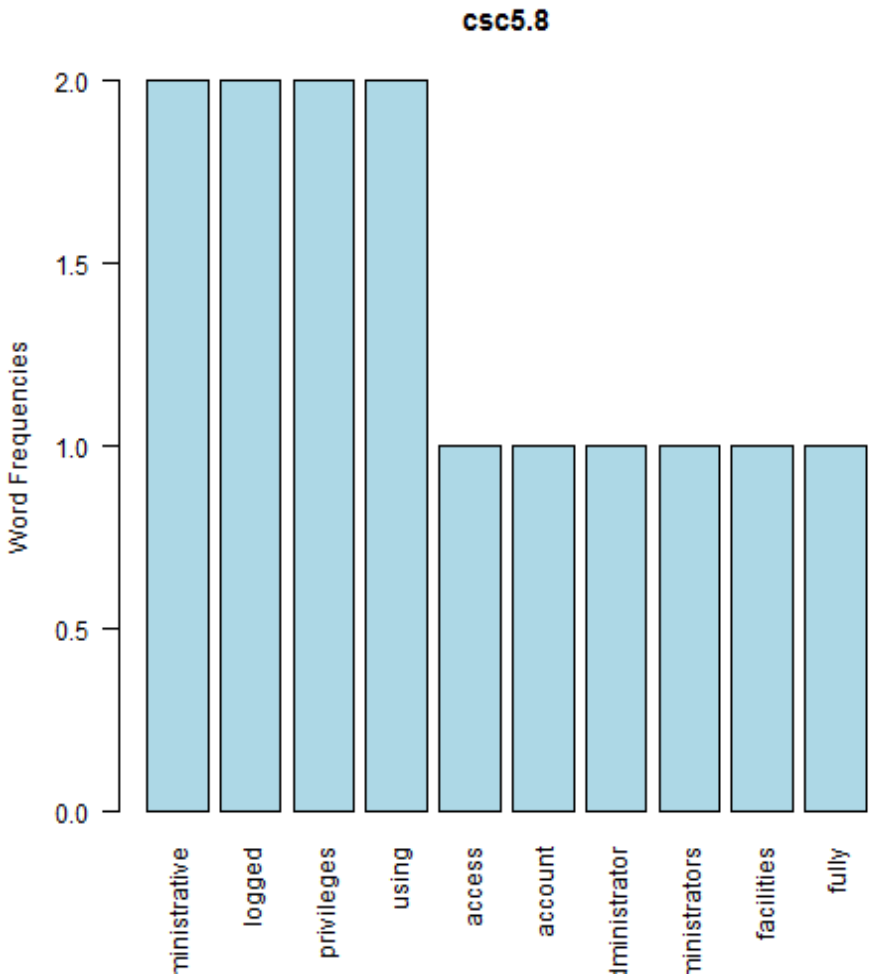


null device 1 [1] “Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).”

CSC 5.8

[1] “administrative + logged”

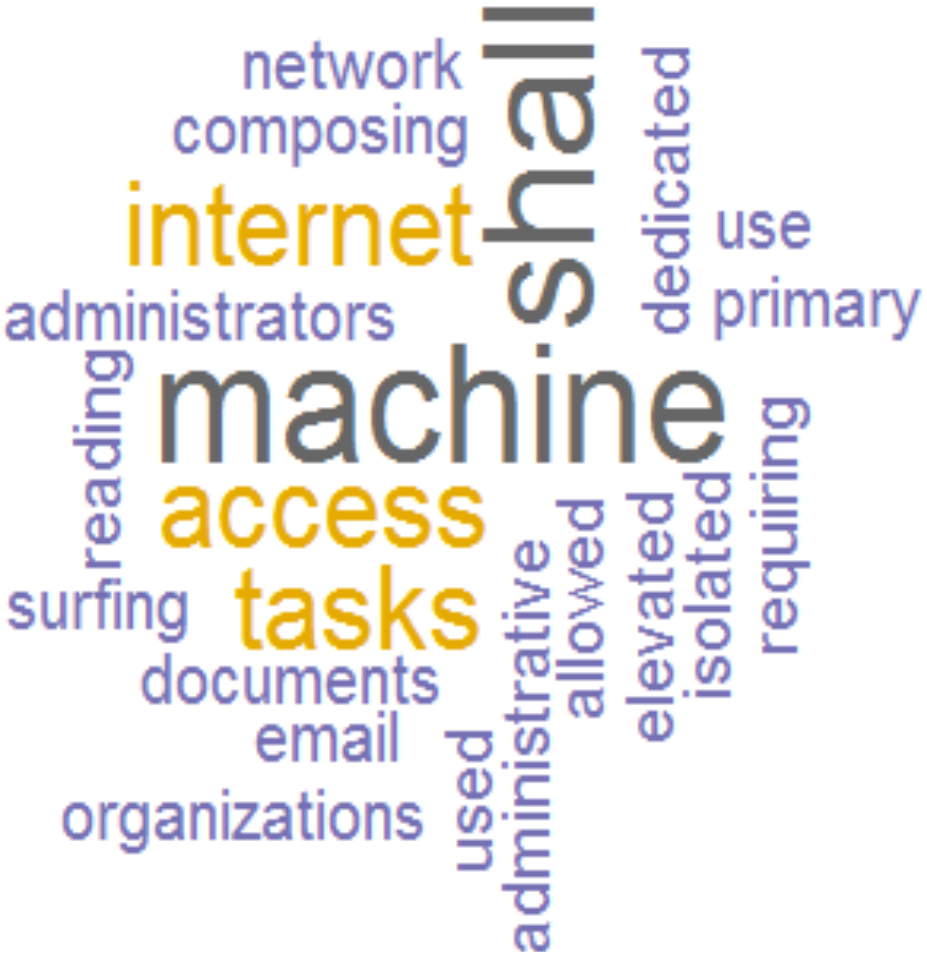
null device 1



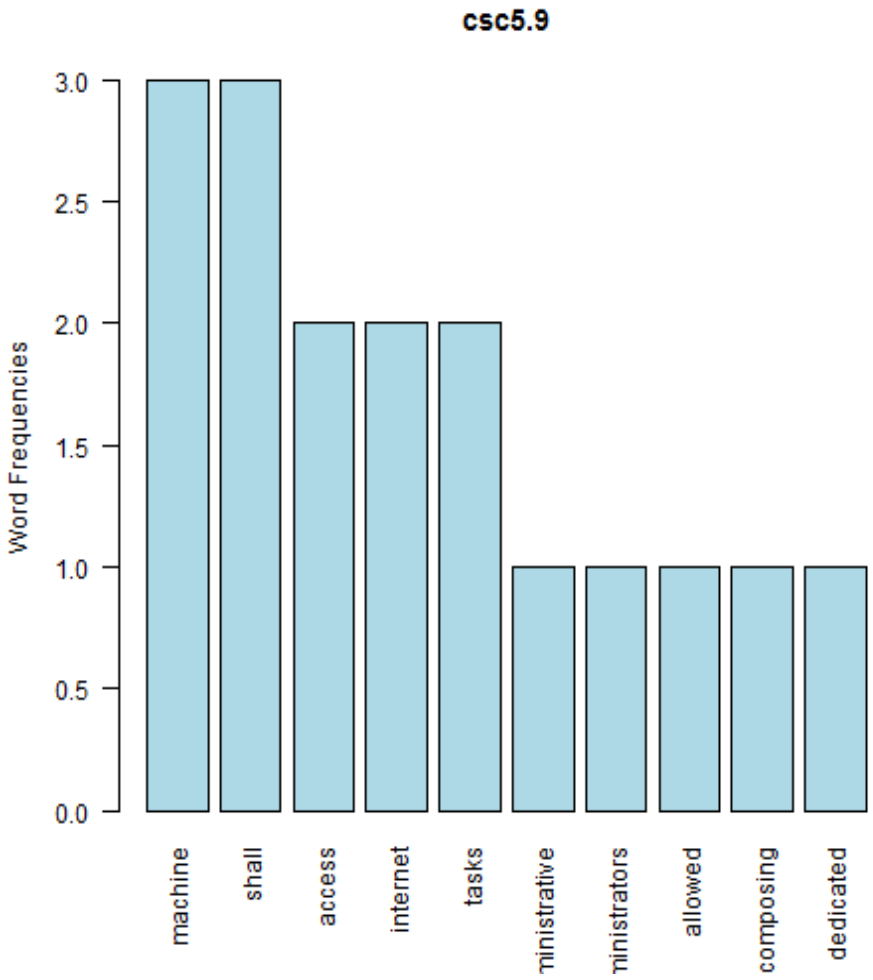
null device 1 [1] "Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems."

CSC 5.9

[1] “machine + shall”



null device 1



null device 1 [1] "Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet."