***Project: Fortifying Foundations: 20 Key Hardening Strategies Across Diverse Systems.***

The project covers important aspects such as configuring specific settings, enabling security features, and ensuring compliance with security best practices.

**Google Cloud Platform**

1. Pg. 192 6.2.5 Ensure 'log-duration' database flag for Cloud SQL PostgreSQL instance is set on 'on.'

It is important to switch on the 'log-duration' flag for Cloud SQL PostgreSQL Instances to make monitoring & Improving performance. When you set 'log-duration' to ‘on’ the system will keep track of how long each statement takes to run, without logging the actual query text. This helps identify statements that are taking longer than normal possibly slowing down your server.

By default, log\_duration is off.

To enable:

Using the Google Cloud Console:

* Visit https://console.cloud.google.com/sql/instances to access the Cloud SQL Instances page.
* Pick the PostgreSQL instance you want to enable the database flag for.
* Select "Edit."
* Scroll down to find the "Flags" section.
* If the 'log\_duration' flag hasn't been previously set on the instance, click "Add item." From the drop-down menu, choose 'log\_duration' and set its value to 'on.'
* Save your changes by clicking "Save."
* Confirm the changes by verifying the 'Flags' section on the 'Overview' page.

Using command line:

* First step is to list all Cloud SQL database instances.

By entering the following command:

gcloud sql instances list

* Second step, is to Configure the 'log\_duration' database flag for each Cloud SQL PostgreSQL database instance with the following command:

gcloud sql instances patch INSTANCE\_NAME --database-flags log\_duration=on

References:

1. https://cloud.google.com/sql/docs/postgres/flags

2. https://www.postgresql.org/docs/9.6/runtime-config-logging.html#GUC-LOG-MIN-

DURATION-STATEMENT

1. Pg. 33 1.8 Ensure that Separation of duties is enforced while assigning service account related roles to users

It's crucial to enforce Separation of Duties when assigning service account-related roles in Google Cloud. This ensures that no single user has both Service Account Admin and Service Account User roles at the same time, reducing the risk of unauthorized access and potential misuse. Separation of duties is a key security principle that helps prevent conflicts, errors, and intentional misuse of privileges, making your environment more secure.

How to Enforce Separation of Duties via Google Cloud Console:

* Navigate to https://console.cloud.google.com/iam-admin/iam.
* Review Assigned Roles Ensuring that no user has both the roles of Service Account Admin and Service Account User assigned simultaneously if they do click the delete bin icon to modify and remove either role.

References:

1. https://cloud.google.com/iam/docs/service-accounts

2. https://cloud.google.com/iam/docs/understanding-roles

3. https://cloud.google.com/iam/docs/granting-roles-to-service-accounts

1. Pg. 108 3.4 Ensure that RSASHA1 is not used for the key-signing key in Cloud DNS DNSSEC

Making sure RSASHA1 isn't used for key-signing in Cloud DNS DNSSEC is super important for keeping your DNS (Domain Name System) safe. RSASHA1 used to be okay, but now it's not so secure. Choosing a strong and recommended algorithm for key signing boosts the overall security of DNSSEC, which is crucial for making sure domain names are resolved correctly.

By default DNSSEC is not enabled.

* Use this command to see that keyType keySigning is not using RSASHA1:

gcloud dns managed-zones describe ZONENAME --format="json(dnsName,dnssecConfig.state,dnssecConfig.defaultKeySpecs)"

* Setting NSSEC must be turned off and enable with a different setting.

To turn off enter the following command:

gcloud dns managed-zones update ZONE\_NAME --dnssec-state off

* Next use this command to switch up the key-signing algorithm by entering the following command: gcloud dns managed-zones update ZONE\_NAME --dnssec-state on --ksk-algorithm KSK\_ALGORITHM --ksk-key-length KSK\_KEY\_LENGTH --zsk-algorithm ZSK\_ALGORITHM --zsk-key-length ZSK\_KEY\_LENGTH --denial-of-existence DENIAL\_OF\_EXISTENCE

References:

1. https://cloud.google.com/dns/dnssec-advanced#advanced\_signing\_options

1. Pg. 121 3.9 Ensure no HTTPS or SSL proxy load balancers permit SSL policies with

weak cipher suites

Making sure that HTTPS or SSL proxy load balancers don't allow weak cipher suites in SSL policies is crucial for keeping your web traffic secure. Weak cipher suites can create vulnerabilities, allowing unauthorized access and risking the integrity of your data. By only allowing strong cipher suites, you improve the confidentiality and security of data sent over HTTPS or SSL proxy load balancers. This approach follows current security standards and helps guard against evolving cyber threats. The GCP default SSL policy is the least secure setting.

**Remediation:**

From Console:

If the TargetSSLProxy or TargetHttpsProxy does not have an SSL policy configured, create a new SSL policy.

* + Go to the SSL Policies page by navigating to https://console.cloud.google.com/net-security/sslpolicies
  + Click on the name of the insecure policy to go to its SSL policy details page.
  + Click EDIT.
  + Set Minimum TLS version to TLS 1.2.
  + Set Profile to Modern or Restricted.
  + If user selects the profile custom, make sure that the following features are disabled:

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

From Command Line:

* For each insecure SSL policy, update it to utilize secure ciphers with the following command:

gcloud compute ssl-policies update NAME [--profile COMPATIBLE|MODERN|RESTRICTED|CUSTOM] --min-tls-version 1.2 [--custom-features FEATURES]

* For each insecure SSL policy, update it to utilize secure ciphers with the following command:

For Target SSL Proxy:

gcloud compute target-ssl-proxies update TARGET\_SSL\_PROXY\_NAME --ssl-policy SSL\_POLICY\_NAME

For Target HTTPS Proxy:

gcloud compute target-https-proxies update TARGET\_HTTPS\_POLICY\_NAME --ssl-policy SSL\_POLICY\_NAME

**References:**

1. https://cloud.google.com/load-balancing/docs/use-ssl-policies

2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

1. Pg 15 1.2 Ensure that multi-factor authentication is enabled for all non-service

accounts

Enabling multi-factor authentication (MFA) for your accounts is like adding an extra layer of security beyond just using a password. It's a bit like having a double lock on your door – even if someone figures out your password, they still need another code or key to get in. This makes it much tougher for unauthorized access. MFA is important because it follows rules, protects important information, and gives you more control over your security. It's like using a special key along with your password, making it harder for bad actors to get into your accounts and keep your personal information safe.

By default, multi-factor is not set, to set it up, you must

* first Identify non-service accounts.
* Secondly Setup multi-factor authentication for each account.

**References:**

1. https://cloud.google.com/solutions/securing-gcp-account-u2f

2. https://support.google.com/accounts/answer/185839

1. Pg 216 6.2.13 Ensure that the 'log\_min\_messages' database flag for Cloud SQL

PostgreSQL instance is set appropriately.

Setting the 'log\_min\_messages' database flag for a Cloud SQL PostgreSQL instance is important for managing the database well. It's like choosing what messages the database should pay attention to. By setting it right, you make sure the database logs the important stuff without filling up with unnecessary details. This helps in keeping an eye on how the database is doing, finding, and fixing problems faster, and saving resources. It's also crucial for security, making sure any suspicious activities are noted.

To enable the 'log\_min\_messages' database flag for a PostgreSQL instance in Google Cloud, you can do it through the Console or the Command Line.

By default log\_min\_error\_statement is ERROR.

Only use 'DEBUG5' carefully, mainly in test environments or when dealing with specific issues that require a lot of details. For actual live systems, go for a simpler setting like 'INFO' or 'NOTICE' to avoid too much unnecessary information.

From Console:

* Visit https://console.cloud.google.com/sql/instances.
* Choose your PostgreSQL instance.
* Click Edit.
* Scroll down to the Flags section.
* To add a new flag, click Add item, select 'log\_min\_messages,' and set the value.
* Save your changes.
* Confirm the changes on the Overview page.

From Command Line:

* To list all instances with the following code:

gcloud sql instances list.

* Configure the 'log\_min\_messages' flag for a specific instance using:

gcloud sql instances patch INSTANCE\_NAME --database-flags

log\_min\_messages=<DEBUG5|DEBUG4|DEBUG3|DEBUG2|DEBUG1|INFO|NOTICE|WARNING|ERROR|LOG|FATAL|PANIC>

**References:**

1. https://cloud.google.com/sql/docs/postgres/flags

2. https://www.postgresql.org/docs/9.6/runtime-config-logging.html#RUNTIME-

CONFIG-LOGGING-WHEN

1. Pg 17 1.3 Ensure that Security Key Enforcement is enabled for all admin

accounts (Manual)

Enabling Security Key Enforcement for admin accounts is crucial for stronger system security. This involves using physical keys alongside passwords, adding a robust layer of defense against common cyber threats. It safeguards sensitive data, ensures compliance with standards, and enhances user accountability. In essence, it acts as a powerful defense mechanism, making unauthorized access more challenging and fortifying overall system security. By default, Security Key Enforcement is not enabled for Organization Administrators.

To enable Security Key Enforcement:

1. Access your platform's security settings.
2. Identify admin accounts.
3. Enable Security Key Enforcement.
4. Configure security keys for each admin account.
5. Test to ensure proper functionality.

**References:**

1. https://cloud.google.com/security-key/

2. https://gsuite.google.com/learn-

more/key\_for\_working\_smarter\_faster\_and\_more\_securely.html

1. Pg 198 6.2.7 Ensure 'log\_statement' database flag for Cloud SQL PostgreSQL

instance is set appropriately.

Configuring the 'log\_statement' database flag right in Cloud SQL PostgreSQL is like choosing how detailed you want your system to log its actions. It's crucial for two main reasons: making sure the system runs smoothly and catching any potential security issues. By setting this flag, you decide how much information you want about the SQL commands your database is handling. This helps in keeping an eye on performance, fixing problems, and making sure no one is doing anything they shouldn't be doing. If you need to track schema changes, consider setting 'log\_statement=ddl.' It is important for maintaining visibility into alterations made to the database structure, aiding in auditing, and ensuring data integrity. The default value for the 'log\_statement' database flag in Cloud SQL PostgreSQL instances is typically set to 'none'.

**Console:**

* + Go to the Cloud SQL Instances page in the Google Cloud Console.
  + Select the PostgreSQL instance.
  + Click Edit.
  + Scroll down to the Flags section.
  + Add a new item, choose 'log\_statement' from the drop-down menu, and set the appropriate value ('none,' 'ddl,' 'mod,' 'all').
  + Save the changes.

**Command Line:**

* + Use the **gcloud** command to configure the 'log\_statement' flag:

gcloud sql instances patch INSTANCE\_NAME --database-flags log\_statement=<ddl|mod|all | none>

**References:**

1. https://cloud.google.com/sql/docs/postgres/flags

2. https://www.postgresql.org/docs/current/runtime-config-

logging.html#RUNTIME-CONFIG-LOGGING-WHAT

1. Pg 47 1.13 Ensure API keys are restricted to use by only specified Hosts and Apps.

It's essential to restrict API keys to specified hosts and apps for security reasons. This measure prevents unauthorized access and potential misuse, ensuring that the keys are only used in trusted environments. This practice reduces the risk of unauthorized access, data breaches, and malicious activities, enhancing the overall security and reliability of the application or system.

By default, Application Restrictions are set to None. When you create an API key it is initially unrestricted by default.

* Navigate to the APIs & Services\Credentials section. https://console.cloud.google.com/apis/credentials
* Click on the API Key Name. The API Key properties will display on a new page.
* In the "Key restrictions" section, set the "Application restrictions" to any of HTTP referrers, IP Addresses, Android Apps, or iOS Apps.
* Click "Save."
* Repeat steps 2-4 for each unrestricted API key.

**References:**

1. https://cloud.google.com/docs/authentication/api-keys

1. Pg 183 6.2.2 Ensure 'log\_error\_verbosity' database flag for Cloud SQL

PostgreSQL instance is set to 'DEFAULT' or stricter.

Make sure your Cloud SQL PostgreSQL's 'log\_error\_verbosity' is set to 'DEFAULT' or stricter. This keeps your system safe by not revealing sensitive info in error logs. It follows standards for protecting data and makes debugging simpler without filling up logs with too much detail. It also helps your system run smoothly and saves storage space.

DEFAULT': Standard level of detail, good for most cases.

'TERSE': Minimal information, keeps things concise.

'VERBOSE': More detailed logs, helpful for in-depth debugging.

It's like picking the level of detail that suits your needs.

I would change it to VERBOSE It will provide a more detailed view in error logs, which can be beneficial for debugging. However, be cautious as it might expose sensitive information.

**Using Console:**

* Navigate to the https://console.cloud.google.com/sql/ in the Google Cloud Console.
* Choose the PostgreSQL instance you want to configure.
* Click on the "Edit" button.
* Scroll down to the FLAG section.
* If 'log\_error\_verbosity' is not set, click "Add item," select 'log\_error\_verbosity' from the dropdown, and set the appropriate value (terse, default, verbose)
* Click "Save" to apply your changes.
* Confirm your changes under Flags on the overview board.

**Using Command Line:**

* List all Cloud SQL database instances:

gcloud sql instances list

* Configure the 'log\_error\_verbosity' flag for each PostgreSQL database instance with the following command:

gcloud sql instances patch INSTANCE\_NAME --database-flags log\_error\_verbosity=<TERSE|DEFAULT|VERBOSE>

**References:**

* 1. https://cloud.google.com/sql/docs/postgres/flags
  2. https://www.postgresql.org/docs/current/runtime-config-logging.html#RUNTIME-CONFIG-LOGGING-WHAT

1. Pg 159 4.11 Ensure that Compute instances have Confidential Computing enabled.

Enabling Confidential Computing on your computer instances is like setting up a strong protective shield around your sensitive data. It ensures that even those with high-level access can't compromise the confidentiality of your personal information, financial records, or business data. This security feature guards against insider threats and allows secure processing of encrypted data, enhancing trust in outsourcing tasks to external providers. By default, Confidential Computing is disabled for Compute instances.

To activate Confidential Computing, it can only be enabled during the instance creation process. Follow these steps:

**Using the Console:**

* Navigate to the VM instances page at https://console.cloud.google.com/compute/instances.
* Click on "CREATE INSTANCE."
* Complete the necessary configuration for your instance.
* In the Confidential VM service section, tick the box that says "Enable the Confidential Computing service on this VM instance."
* Press "Create."

From Command Line:

* Create a new instance with Confidential Compute enabled, using the following command:

gcloud beta compute instances create INSTANCE\_NAME --zone ZONE -- confidential-compute --maintenance-policy=TERMINATE

**References:**

1. https://cloud.google.com/compute/confidential-vm/docs/creating-cvm-instance 2. https://cloud.google.com/compute/confidential-vm/docs/about-cvm

3. https://cloud.google.com/confidential-computing

1. Pg 47 1.13 Ensure API keys are restricted to use by only specified Hosts and Apps

Making sure API keys only work for certain hosts and apps is super important. It stops bad guys from getting in, keeps your important data safe, and follows security rules. It also prevents using too many resources and makes it easier to find out where a problem came from. So, by restricting API keys, you're giving your apps an extra layer of protection. By default, Application Restrictions are set to None.

To Change from Console:

* Navigate to APIs & Services\Credentials at https://console.cloud.google.com/apis/credentials.
* In the API Keys section, click on the name of the API Key. This opens the API Key properties on a new page.
* In the Key restrictions section, choose from options like HTTP referrers, IP Addresses, Android Apps, or iOS Apps.
* Click Save.
* Repeat steps 2-4 for every API key without restrictions.

References:

* + 1. https://cloud.google.com/docs/authentication/api-keys

1. Pg 49 1.14 Ensure API keys are restricted to only APIs that application needs access Making sure API keys only work with the stuff your app really needs is super important. It keeps bad guys from getting in where they shouldn't, prevents using too much computer power, and makes it easier to fix problems if something goes wrong. This way, you're only giving your app the keys to the doors it actually needs to open. By default, API restrictions are set to None.

Using the console, follow these steps to secure your API keys:

* Visit https://console.cloud.google.com/apis/credentials and go to APIs & Services\Credentials.
* In the API Keys section, click on the API Key Name. The API Key properties will appear on a new page.
* In the Key restrictions section, go to API restrictions.
* Use the Select API drop-down to pick the API you want.
* Click Save.

**References:**

1. https://cloud.google.com/docs/authentication/api-keys 2. https://cloud.google.com/apis/docs/overview

1. Pg 51 1.15 Ensure API keys are rotated every 90 days

Regularly changing API keys every 90 days is critical for security. It prevents malicious users from exploiting a key for an extended period, conforms to security best practices, and adapts to emerging threats. This practice is essential for minimizing the consequences of a compromised key, improving accountability, and ensuring ongoing security. There is no option to automatically regenerate (rotate) API keys periodically.

To enable API key rotation:

* Navigate to APIs & Services\Credentials at https://console.cloud.google.com/apis/credentials?project=clever-guard-405216
* In the API Keys section, select the API Key Name. The API Key properties will appear on a new page.
* Click on REGENERATE KEY to rotate the API key.
* Save the changes.

**References:**

* 1. https://developers.google.com/workspace/guides/create-credentials
  2. https://hub.steampipe.io/mods/turbot/gcp\_compliance/controls/control.cis\_v120\_1\_15?context=benchmark.cis\_v120/benchmark.cis\_v120\_1

1. Pg 118 3.8 Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network

Enabling VPC Flow Logs for each subnet in a VPC network is crucial for security and monitoring. It provides detailed information about network traffic, helping detect and respond to security threats. Flow logs aid in troubleshooting network issues, ensuring compliance, and are valuable for auditing. They also assist in capacity planning and optimizing network performance. In essence, VPC Flow Logs enhance visibility, security, and operational efficiency within your virtual network. When a new VPC network subnet is created, Flow Logs are initially set to the "Off" position by default.

To activate Flow Logs for a network subnet, take the following steps:

Using the Console:

* Visit the VPC network GCP Console at https://console.cloud.google.com/networking/networks/list.
* Select a subnet by clicking on its name to access the Subnet details page.
* Click the EDIT button.
* Turn on Flow Logs.
* Save your changes.

Using Command Line:

* To enable Flow Logs for a network subnet, use the command:

gcloud compute networks subnets update [SUBNET\_NAME] --region [REGION] --enable-flow-logs

**References:**

* 1. https://cloud.google.com/vpc/docs/using-flow-logs#enabling\_vpc\_flow\_logging
  2. https://cloud.google.com/vpc/

1. Pg 125 3.10 Ensure Firewall Rules for instances behind Identity Aware Proxy (IAP) only allow the traffic from Google Cloud Loadbalancer (GCLB) Health Check and Proxy Addresses

Make sure the firewall rules for Identity Aware Proxy (IAP)-protected instances only allow traffic from Google Cloud Load Balancer (GCLB) Health Check and Proxy Addresses. This keeps things safe, helps IAP work right, and stops certain kinds of cyber attacks. By default all traffic is allowed.

To configure,

* go to Cloud Console, then VPC network, and Firewall rules.
* Check the boxes for these rules:

default-allow-http

default-allow-https

default-allow-internal

* Click Delete.
* Create a new rule with these details:

Name: allow-iap-traffic

Targets: All instances in the network

Source IP ranges (press Enter after each):

130.211.0.0/22

35.191.0.0/16

* For CIS Controls, select "Specified protocols and ports" and add "tcp:805". Click Create when you're done updating.

**References:**

* 1. https://hub.steampipe.io/mods/turbot/gcp\_compliance/controls/control.cis\_v120\_3\_10?context=benchmark.cis\_v120/benchmark.cis\_v120\_3
  2. https://paper.bobylive.com/Security/CIS/CIS\_Google\_Cloud\_Platform\_Foundation\_Benchmark\_v1\_3\_0.pdf

1. Pg 154 4.9 Ensure that Compute instances do not have public IP addresses

It's vital for security that Compute instances don't have public IP addresses. This minimizes the risk of cyber threats, unauthorized access, and unnecessary costs. Following this approach aligns with the principle of least privilege, enhances overall security, and may be required for compliance. By default, Compute instances have a public IP address.

To remove public IP addresses from a Compute instance, follow these steps:

**Using the Console:**

* Visit the VM instances page at https://console.cloud.google.com/compute/instances.
* Click on the instance name to access the Instance detail page.
* Click Edit.
* For each Network interface, ensure that External IP is set to None.
* Click Done and then Save.

**Using Command Line:**

* Describe the instance properties:

gcloud compute instances describe INSTANCE\_NAME --zone=ZONE

* Identify the access config name containing the external IP address.
* Delete the access config:

gcloud compute instances delete-access-config INSTANCE\_NAME --zone=ZONE --access-config-name "ACCESS\_CONFIG\_NAME"

**References:**

* 1. https://paper.bobylive.com/Security/CIS/CIS\_Google\_Cloud\_Platform\_Foundation\_Benchmark\_v1\_3\_0.pdf
  2. https://cloud.google.com/load-balancing/docs/backend-service#backends\_and\_external\_ip\_addresses

1. Pg 61 2.3 Ensure that retention policies on log buckets are configured using Bucket Lock

Using Bucket Lock to set retention policies on log buckets is like putting a strong lock on your important records. It makes sure that once data is saved, it can't be deleted until a certain time has passed. This helps keep a reliable record for checks and investigations, follows the rules, and adds extra protection against accidental or intentional data removal. By default, storage buckets used as log sinks do not have retention policies and Bucket Lock configured.

Using the Console:

* Make sure that sinks are configured for all Log entries.
* Navigate to the Cloud Storage browser at https://console.cloud.google.com/storage/browser/<BUCKET\_NAME>.
* Access the Bucket Lock tab at the top.
* In the Retention policy section, click Add Duration, input the desired retention period, and click Save policy.
* Set the Lock status for this retention policy to Locked.

Using Command Line:

* To view all sinks linked to storage buckets:

gcloud logging sinks list --folder=FOLDER\_ID | --organization=ORGANIZATION\_ID | --project=PROJECT\_ID

* For each storage bucket listed above, establish a retention policy and lock it:

gsutil retention set [TIME\_DURATION] gs://[BUCKET\_NAME]

gsutil retention lock gs://[BUCKET\_NAME]

**References:**

1. https://cloud.google.com/storage/docs/bucket-lock

2. https://cloud.google.com/storage/docs/using-bucket-lock

1. Pg 97 2.12 Ensure that Cloud DNS logging is enabled for all VPC networks.

Enabling Cloud DNS logging for all VPC networks is essential. It provides visibility into DNS activity, aiding security monitoring and compliance. In the event of incidents, DNS logs support forensic analysis and incident response. Additionally, it assists in troubleshooting, anomaly detection, and ensuring resource accountability. Cloud DNS logging is disabled by default on each network.

To enable Cloud DNS logging for all VPC networks, follow these steps:

From Command Line:

Use the following command to enable Cloud DNS logging for a specific VPC network:

gcloud dns policies create enable-dns-logging --enable-logging --description="Enable DNS Logging" --networks=VPC\_NETWORK\_NAME

**References:**

* 1. https://cloud.google.com/dns/docs/monitoring
  2. https://www.tenable.com/audits/items/CIS\_Google\_Cloud\_Platform\_v1.2.0\_L1.audit:5f2ad1e79c6d2832c664d284a9a6e183

1. Pg 58 2.2 Ensure that sinks are configured for all log entries.

Setting up sinks for all log entries is crucial. It ensures thorough monitoring, centralizes logs for easy management, meets security compliance, aids quick incident response, optimizes resource usage, and allows customization based on specific needs.

Using the Console:

* Open Logging/Logs at https://console.cloud.google.com/logs/viewer.
* Click the down arrow on the rightmost corner of the Filter Bar and select Convert to Advanced Filter.
* This changes the Filter Bar to the Advanced Filter Bar.
* Make sure the Advanced Filter field is empty to capture all logs.
* Click Submit Filter to see all logs.
* Click Create Sink on the right-side menu.
* Fill in the fields and click Create Sink.

To set up a sink for exporting all log entries to a Google Cloud Storage bucket, follow these commands:

* + gcloud logging sinks create <sink-name> storage.googleapis.com/DESTINATION\_BUCKET\_NAME

For sinks covering a folder or organization, including all projects, use:

* gcloud logging sinks create <sink-name> storage.googleapis.com/DESTINATION\_BUCKET\_NAME --include-children --folder=FOLDER\_ID | --organization=ORGANIZATION\_ID

**References:**

1. https://cloud.google.com/logging/docs/reference/tools/gcloud-logging 2. https://cloud.google.com/logging/quotas

3. https://cloud.google.com/logging/docs/export/

**Amazon Web Services**

1. Pg 63 1.19 Ensure that all the expired SSL/TLS certificates stored in AWS IAM are removed.

Removing expired SSL/TLS certificates from AWS IAM is important for security. It helps prevent issues, ensures compliance, and keeps our systems safe. By default, expired certificates won't get deleted.

Using Command Line:

* To remove an expired certificate, use the following command:

aws iam delete-server-certificate --server-certificate-name <CERTIFICATE\_NAME>

**Deleting a Certificate using the Console:**

* Navigate to the ACM console at https://console.aws.amazon.com/acm/.
* From the list of certificates, check the box next to the ACM certificate you want to delete.
* Click on the "Delete" option.

**References:**

* 1. https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-delete.html
  2. https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html

2. Pg 98 3.1 Ensure CloudTrail is enabled in all regions

Enabling CloudTrail everywhere is important for complete AWS logs, better security monitoring, and easier incident response. It helps with rules, forensic analysis, and gives insights across all AWS areas uniformly.

**Console Steps:**

* Log in to the AWS Management Console and access the CloudTrail console at https://console.aws.amazon.com/cloudtrail.
* Click on "Trails" in the left menu.
* If asked, select "Get Started Now" and then choose "Add new trail."
  1. Provide a name for the trail.
  2. Turn on "Apply trail to all regions."
  3. Specify an S3 bucket name.
  4. Click on Create.
* If there are existing trails, pick the one for global logging.
* Click the edit icon (pencil) next to "Apply trail to all regions," set it to Yes, and save.
* Click the edit icon (pencil) next to "Management Events," set "Read/Write Events" to all and save.

**References:**

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-concepts.html#cloudtrail-concepts-management-events
2. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/logging-

management-and-data-events-with-

cloudtrail.html?icmpid=docs\_cloudtrail\_console#logging-management-events

1. Pg 101 3.2 Ensure CloudTrail log file validation is enabled.

Enabling CloudTrail log file validation is crucial for ensuring the security and reliability of your AWS log files. It helps prevent tampering and ensures the information in your logs is trustworthy. By default, is Not Enabled.

To turn on log file validation for a specific trail, follow these steps:

**Using the AWS Console:**

* Log in to the AWS Management Console https://console.aws.amazon.com/cloudtrail.
* Go to Trails in the left menu.
* Click on the trail you want.
* Under the S3 section, click the edit icon (pencil).
* Select Advanced.
* Choose "Yes" for Enable log file validation.
* Save your changes.

**Using the Command Line:**

* Run this command:

aws cloudtrail update-trail --name <trail\_name> --enable-log-file-validation

**References:**

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file- validation-enabling.html

1. Pg 76 2.1.2 Ensure S3 Bucket Policy is set to deny HTTP requests.

Setting the S3 bucket policy to deny HTTP requests is crucial for security. It ensures that data going to and from the bucket is encrypted, protecting sensitive information. This practice aligns with standards, prevents certain attacks, and builds trust by showing a commitment to secure data handling. By default, S3 buckets allow both HTTP and HTTPS requests.

**From Command Line:**

**From Command Line:**

* Export the current bucket policy to a JSON file:

aws s3api get-bucket-policy --bucket <bucket\_name> --query Policy --output text > policy.json

* Modify the **policy.json** file by adding the following statement:

{

"Sid": "<optional>",

"Effect": "Deny",

"Principal": "\*",

"Action": "s3:GetObject",

"Resource": "arn:aws:s3:::<bucket\_name>/\*",

"Condition": {

"Bool": {

"aws:SecureTransport": "false"

}

}

}

* Apply the modified policy back to the S3 bucket:

aws s3api put-bucket-policy --bucket <bucket\_name> --policy file://policy.json

**References:**

* 1. https://aws.amazon.com/premiumsupport/knowledge-center/s3-bucket-policy- for-config-rule/

1. Pg 60 1.18 Ensure IAM instance roles are used for AWS resource access from instances.

Using IAM instance roles for AWS resource access improves security by avoiding long-term credential storage on instances, providing safer and simpler access management.

To fix an instance without an IAM role:

* create a new IAM role in AWS IAM with the necessary permissions.
* Then, launch a new instance in the AWS console, making sure to select the newly created role.
* After shutting down both the old and new instances, detach the disks from both. Attach the disks from the old instance to the new one, and restart.
* Now, the new instance has the same setup with the associated IAM role.

**References:**

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon- ec2.html

1. Pg 73 2.1.1 Ensure all S3 buckets employ encryption-at-rest.

Enabling encryption-at-rest in all S3 buckets is vital for data security, compliance, and maintaining confidentiality. It proactively mitigates risks, builds customer trust, prevents data tampering, adheres to cloud security standards, and reduces insider threat impact.

Encryption-at-rest for S3 buckets is not enabled by default in AWS. AWS account owners or administrators must manually configure encryption settings for individual S3 buckets. According to Amazon “Starting January 5, 2023, all new object uploads to Amazon S3 are automatically encrypted at no additional cost and with no impact on performance.”

To fix, go to the AWS S3 console:

* Log in at https://console.aws.amazon.com/s3/.
* Select the bucket by checking the box.
* Click 'Properties.'
* Choose 'Default Encryption.'
* Select either AES-256 or AWS-KMS.
* Save the changes.
* Repeat for all buckets without encryption in your AWS account.

From the command line:

* Execute either of the following:

aws s3api put-bucket-encryption --bucket <bucket name> --server-side-encryption-configuration '{"Rules": [{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm": "AES256"}}]}'

* The other option is to enter the following command:

aws s3api put-bucket-encryption --bucket <bucket name> --server-side- encryption-configuration '{"Rules": [{"ApplyServerSideEncryptionByDefault": {"SSEAlgorithm": "aws:kms","KMSMasterKeyID": "aws/s3"}}]}'

**References:**

1. https://docs.aws.amazon.com/AmazonS3/latest/user-guide/default-bucket- encryption.html

2. https://docs.aws.amazon.com/AmazonS3/latest/dev/bucket- encryption.html#bucket-encryption-related-resources

1. Pg 201 5.4 Ensure routing tables for VPC peering are "least access"

To ensure "least access," follow best practices by defining explicit route entries, avoiding default routes, using specific IP ranges, regularly reviewing, and updating routes, and implementing logging and monitoring for VPC peering connections. These practices help maintain a secure and efficient network configuration.

To fix, adjust route table entries to allow the least necessary subnets or hosts for the intended peering purpose.

* Identify non-compliant route tables with excessive access:

aws ec2 describe-route-tables --filter "Name=vpc-id,Values=<vpc\_id>" --query "RouteTables[\*].{RouteTableId:RouteTableId, VpcId:VpcId, Routes:Routes, AssociatedSubnets:Associations[\*].SubnetId}"

* Delete non-compliant routes for each identified route table:

aws ec2 delete-route --route-table-id <route\_table\_id> --destination-cidr-block <non\_compliant\_destination\_CIDR>

**References:**

1. https://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering- configurations-partial-access.html

2. https://docs.aws.amazon.com/cli/latest/reference/ec2/create-vpc-peering- connection.html

1. Pg 82 2.1.4 Ensure all data in Amazon S3 has been discovered, classified and secured when required.

AWS does not enforce a default configuration for discovering, classifying, and securing data in Amazon S3.

It's crucial to discover, classify, and secure data in Amazon S3 to ensure sensitive information is protected, comply with regulations, prevent unauthorized access, and maintain a robust security posture.

To enable and configure Amazon Macie, follow these steps:

**Enable Macie:**

* Log in to the Macie console at https://console.aws.amazon.com/macie/.
* Click "Get started."
* Click "Enable Macie."

**Setup a Repository for Discovery Results:**

* Under "Settings," click "Discovery results."
* Ensure "Create bucket" is selected.
* Create a unique bucket, ensuring it starts with a lowercase letter or number.
* Click "Advanced."
* Select "Yes" to block all public access.
* Specify an AWS KMS key for encryption.
* Click "Save."

**Create a Job to Discover Sensitive Data:**

* Click "S3 buckets" in the left pane.
* Select the buckets for analysis.
* Click "Create job."
* Choose "Quick create."
* Enter a name and optional description.
* Click "Next."
* In the "Review and create" step, click "Submit."

**Review Findings:**

* Click "Findings" in the left pane.
* To view details, click any field other than the checkbox for the specific finding.

You can also use a third-party company tool to protect and manage s3 data. If a third-party company is used make sure to follow their instructions to enable.

**References:**

1. https://aws.amazon.com/macie/getting-started/

2. https://docs.aws.amazon.com/workspaces/latest/adminguide/data-

protection.html

3. https://docs.aws.amazon.com/macie/latest/user/data-classification.html

4. https://aws.amazon.com/about-aws/whats-new/2020/11/third-party-software-for-amazon-s3-available-in-amazon-s3-management-console-powered-by-aws-marketplace/

1. Pg 69 1.21 Ensure IAM users are managed centrally via identity federation or AWS Organizations for multi-account environments.

Centralized management improves efficiency, maintains consistent security policies, and enhances overall security by offering greater control and visibility over user access in multi-account environments. Users can be centralized by connecting with an external identity provider or using AWS Organizations

**Remediating** the issue depends on how the organization implemented identity federation or AWS Organizations. Make sure no non-service IAM users or non-root accounts exist outside the centrally managed account.

**References:**

* 1. https://aws.amazon.com/iam/identity-center/

1. Pg 90 2.2.1 Ensure EBS volume encryption is enabled.

Enabling EBS volume encryption is important to protect your data from unauthorized access and ensure compliance with security standards.

EBS volume encryption is not enabled by default.

To change configuration via console:

* Sign in to the AWS Management Console and navigate to the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
* In Account attributes, select EBS encryption.
* Choose Manage.
* Enable the checkbox.
* Click Update EBS encryption.
* Repeat these steps for each region where the change is needed.

Execute the command:

**aws --region <region> ec2 enable-ebs-encryption-by-default**.

* Confirm that "EbsEncryptionByDefault": true is shown.
* Repeat this process for each region where the change is necessary.

**References:**

1. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html

2. https://aws.amazon.com/blogs/aws/new-opt-in-to-default-encryption-for-new-

ebs-volumes/

1. Pg 13 1.1 Maintain current contact details.

Keeping contact details up to date is crucial for timely communication and business continuity. Communication breakdowns, missed opportunities, and delays in emergency responses can occur if contact details are not correctly set up. If account is being created make sure to input up to date information and in case of any changes to update information, follow the next steps:

Log in to the AWS Management Console and go to the Billing and Cost Management console at https://console.aws.amazon.com/billing/home#/.

* Click on your account name in the navigation bar, then select My Account.
* Choose Edit next to Account Settings.
* Click Edit next to the field you want to update.
* Enter your changes and click Save changes.
* Click Done after making changes.
* To update contact info, click Edit under Contact Information.
* Type your updated info in the fields you want to change and click Update.

**References:**

* 1. https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/manage-account- payment.html#contact-info

1. Pg 15 1.2 Ensure security contact information is registered.

Security contact registration is vital for quick incident response, staying informed about threats, meeting regulations, and collaborating efficiently with others to maintain a secure environment.

To set up security contact information from console:

* Click your account name in the top-right corner.
* Choose "My Account" from the menu.
* Scroll down to "Alternate Contacts."
* Enter your security contact details in the "Security" section.

**Refrences:**

* 1. https://docs.bridgecrew.io/docs/iam\_19

1. Pg 17 1.3 Ensure security questions are registered in the AWS account.

Registering security questions in the AWS account default configuration is important for enhancing account security. Security questions provide an additional layer of authentication, helping to verify the identity of users and prevent unauthorized access. This simple but effective measure contributes to overall account protection and aligns with best practices for securing AWS accounts.

To set up security questions for your AWS account:

* Log in as the 'root' user.
* Click on your account name in the top-right corner.
* Choose "My Account" from the menu.
* Scroll down to "Configure Security Questions."
* Click "Edit," select and answer three questions.
* Save your changes and securely store the questions and answers.

**References:**

1. https://docs.aws.amazon.com/config/latest/developerguide/operational-best-practices-for-cis\_aws\_benchmark\_level\_2.html
2. https://hub.steampipe.io/mods/turbot/aws\_compliance/controls/control.cis\_v130\_1\_3?context=benchmark.cis\_v130/benchmark.cis\_v130\_1
3. Pg 126 3.10 Ensure that Object-level logging for write events is enabled for S3 bucket.

By default, CloudTrail trails don't log data events and so it is recommended to enable Object-level logging for S3 buckets.

Enabling object-level logging for write events in an S3 bucket is crucial for auditing and tracking changes, providing a detailed trail of modifications for forensic analysis. It helps organizations meet compliance requirements, enhances security monitoring, and enables swift incident response by detecting and addressing unauthorized or accidental data modifications.

To enable object-level logging for write events in an S3 bucket from the AWS Management Console:

* Go to the S3 dashboard https://console.aws.amazon.com/s3/.
* Click on the desired bucket under "Buckets" in the left panel.
* Navigate to the "Properties" tab to access bucket configuration.
* Under "Object-level logging," enter or select a CloudTrail name and ensure the "Write event" checkbox is selected.
* Repeat these steps for other S3 buckets as needed.

References:

* 1. https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-cloudtrail- events.html

1. Pg 129 3.11 Ensure that Object-level logging for read events is enabled for S3 bucket.

By default, CloudTrail trails don't log data events and so it is recommended to enable Object-level logging for S3 buckets.

Enabling read event logging in an S3 bucket is vital for tracking data access, ensuring compliance, and quickly identifying unauthorized activity. It strengthens overall security by maintaining a clear record of who reads data from the bucket.

To enable read event logging in an S3 bucket from the AWS Management Console:

* Log in to the AWS Management Console and go to the S3 dashboard https://console.aws.amazon.com/s3/.
* In the left panel, click "Buckets," then choose the S3 bucket you want.
* Click on "Properties" to view the bucket configuration.
* Under "Object-level logging," enter the CloudTrail name to record activity. You can use an existing CloudTrail or create a new one https://console.aws.amazon.com/cloudtrail/.
* Once CloudTrail is selected, tick the "Read event" checkbox to enable object-level logging for read events.
* Repeat these steps for other S3 buckets as needed.

**References:**

* 1. https://docs.aws.amazon.com/AmazonS3/latest/user-guide/enable-cloudtrail- events.html

1. Pg 80 2.1.3 Ensure MFA Delete is enable on S3 buckets.

Enabling MFA Delete on S3 buckets is vital because it adds an extra step of multi-factor authentication, preventing accidental or unauthorized data deletions and enhancing overall data security.

To enable MFA Delete on an S3 bucket using the AWS CLI:

* Open the command line interface.
* Run the command:

aws s3api put-bucket-versioning --profile your-root-profile --bucket Your\_Bucket\_Name --versioning-configuration Status=Enabled,MFADelete=Enabled --mfa "arn:aws:iam::aws\_account\_id:mfa/root-account-mfa-device passcode**"**.

**References:**

* https://docs.aws.amazon.com/AmazonS3/latest/dev/Versioning.html#MultiFactor AuthenticationDelete
* https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMFADelete.html
* https://aws.amazon.com/blogs/security/securing-access-to-aws-using-mfa-part-3/

1. Pg 181 4.13 Ensure a log metric filter and alarm exist for route table changes.

Blocking public access to S3 buckets is important to keep your data safe. It prevents others from getting unauthorized access to your information, reducing the risk of data leaks or security breaches.

To set up monitoring for route table changes in AWS, follow these steps:

* Create a metric filter using the provided filter pattern for route table changes in the CloudTrail Logs.
* Establish an SNS topic to be notified by the alarm.
* Create an SNS subscription for the topic.
* Develop an alarm associated with the CloudWatch Logs Metric Filter and the SNS topic.

Ensure to customize the metric and namespace names as needed. This process enhances security by providing real-time alerts for route table changes in your AWS environment.

**References:**

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-

log-files-from-multiple-regions.html

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-

for-cloudtrail.html

1. Pg 153 4.6 Ensure a log metric filter and alarm exist for AWS Management Console authentication failures.

Setting up a log metric filter and alarm for AWS Management Console authentication failures is crucial for real-time monitoring. It helps quickly detect and respond to failed login attempts, reducing the risk of unauthorized access or brute force attacks. This proactive monitoring ensures the security of AWS Management Console access by providing timely alerts on authentication failures.

To address AWS Management Console login failures, follow these steps:

* Create Metric Filter:

aws logs put-metric-filter --log-group-name "<cloudtrail\_log\_group\_name>" --filter-name "<console\_signin\_failure\_metric>" --metric-transformations metricName="<console\_signin\_failure\_metric>",metricNamespace='CISBenchmark',metricValue=1 --filter-pattern '{ ($.eventName = ConsoleLogin) && ($.errorMessage = "Failed authentication") }'

* Create SNS Topic:

aws sns create-topic --name <sns\_topic\_name>

* Create SNS Subscription:

aws sns subscribe --topic-arn <sns\_topic\_arn> --protocol <protocol\_for\_sns> --notification-endpoint <sns\_subscription\_endpoints>

* Create Alarm:

aws cloudwatch put-metric-alarm --alarm-name "<console\_signin\_failure\_alarm>" --metric-name "<console\_signin\_failure\_metric>" --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --namespace 'CISBenchmark' --alarm-actions <sns\_topic\_arn>

**References:**

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-

log-files-from-multiple-regions.html

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-

for-cloudtrail.html

1. Pg 189 4.15 Ensure a log metric filter and alarm exists for AWS Organizations changes

It's crucial to have a log metric filter and alarm for AWS Organizations changes to promptly detect and respond to any modifications in the organizational structure. This enhances security by providing real-time monitoring and alerts for potential unauthorized changes or security incidents.

Following to setup the metric filter, alarm, SNS topic, and subscription:

* **Create Metric Filter:**

aws logs put-metric-filter --log-group-name <cloudtrail\_log\_group\_name> --filter-name `<organizations\_changes>` --metric-transformations metricName= `<organizations\_changes>` ,metricNamespace='CISBenchmark',metricValue=1 --filter-pattern '{ ($.eventSource = organizations.amazonaws.com) && (($.eventName = "AcceptHandshake") || ($.eventName = "AttachPolicy") || ... || ($.eventName = "UpdateOrganizationalUnit")) }'

* **Create SNS Topic:**

aws sns create-topic --name <sns\_topic\_name>

* **Create SNS Subscription:**

aws sns subscribe --topic-arn <sns\_topic\_arn> --protocol <protocol\_for\_sns> --notification-endpoint <sns\_subscription\_endpoints>

* **Create Alarm:**

aws cloudwatch put-metric-alarm --alarm-name `<organizations\_changes>` --metric-name `<organizations\_changes>` --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --namespace 'CISBenchmark' --alarm-actions <sns\_topic\_arn>

**References:**

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms- for-cloudtrail.html

2. https://docs.aws.amazon.com/organizations/latest/userguide/orgs\_security\_incide nt-response.html

1. 4.2 Ensure a log metric filter and alarm exist for Management Console sign-in without MFA.

Setting up a log metric filter and alarm for Management Console sign-ins without MFA is vital for quickly identifying and responding to potential security threats. This ensures enhanced security by actively monitoring and alerting on unauthorized access attempts lacking multi-factor authentication. Enabling the log metric filter and alarm for Management Console sign-ins without MFA is not automatic; you need to configure.

* **Create Metric Filter:**

aws logs put-metric-filter --log-group-name <cloudtrail\_log\_group\_name> --filter-name `<no\_mfa\_console\_signin\_metric>` --metric-transformations metricName= `<no\_mfa\_console\_signin\_metric>` ,metricNamespace='CISBenchmark',metricValue=1 --filter-pattern '{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") }'

* + or (To reduce false positives in case Single Sign-On (SSO) is used in the organization):

aws logs put-metric-filter --log-group-name <cloudtrail\_log\_group\_name> --filter-name `<no\_mfa\_console\_signin\_metric>` --metric-transformations metricName= `<no\_mfa\_console\_signin\_metric>` ,metricNamespace='CISBenchmark',metricValue=1 --filter-pattern '{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }'

* **Create SNS Topic:**

aws sns create-topic --name <sns\_topic\_name>

* **Create SNS Subscription:**

aws sns subscribe --topic-arn <sns\_topic\_arn> --protocol <protocol\_for\_sns> --notification-endpoint <sns\_subscription\_endpoints>

* **Create Alarm:**

aws cloudwatch put-metric-alarm --alarm-name `<no\_mfa\_console\_signin\_alarm>` --metric-name `<no\_mfa\_console\_signin\_metric>` --statistic Sum --period 300 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --evaluation-periods 1 --namespace 'CISBenchmark' --alarm-actions <sns\_topic\_arn>

**References:**

1. https://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/viewin g\_metrics\_with\_cloudwatch.html
2. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/receive-cloudtrail-

log-files-from-multiple-regions.html

1. https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-

for-cloudtrail.html

**Apple iOS 14 & iPadOS**

* 1. Pg 52 2.3.1 Ensure 'Managed Safari Web Domains' is `Configured`

Configuring "Managed Safari Web Domains" is crucial for organizations to control and limit access to approved websites, enhancing security. It helps prevent potential security risks and ensures a focused and productive browsing environment for users.

Follow these steps in the Configuration Profile:

* Access Apple Configurator.
* Open the Configuration Profile.
* Navigate to the Domains tab in the left windowpane.
* Input the relevant URL pattern(s) under Managed Safari Web Domains in the right windowpane.
* Deploy the updated Configuration Profile

**References:**

* https://www.tenable.com/audits/items/CIS\_Apple\_iOS\_11\_End\_User\_Owned\_L1\_v1.0.0-AirWatch.audit:aeb442c9f941c9886b4816cff319616e
* https://support.apple.com/guide/deployment/domains-payload-settings-depb4c146c2e/web
  1. Pg 66 2.5.1 Ensure 'VPN' is 'Configured'

Setting up a virtual private network (VPN) is essential as it encrypts data in transit and relies on trusted network services like DNS, effectively reducing the risk of exploitation by malicious actors and ensuring the security of the connected device and its data.

To configure:

**Using Apple Configurator:**

* Open Apple Configurator.
* Access the Configuration Profile.
* Click on the VPN tab in the left windowpane.
* Enter the appropriate VPN configuration in the right windowpane.
* Deploy the Configuration Profile.

**From the Device:**

* Open Settings.
* Go to General.
* Tap VPN.
* Enter the necessary VPN configuration.

**References:**

* + 1. https://support.apple.com/guide/deployment/vpn-settings-overview-dep2d2adb35d/web
  1. Pg 72 2.7.1 Ensure 'Notification Settings' are configured for all 'Managed Apps'

Setting up 'Notification Settings' for all 'Managed Apps' is crucial to maintain a consistent and well-controlled user experience. This ensures efficient communication, boosts productivity, and improves the overall management of applications on the device.

To configure:

* In Settings > Notifications, choose Lock Screen display: Count, Stack, or List.
* Adjust layouts by pinching notifications on the Lock Screen.
* Schedule a summary in Scheduled Summary.
* Control notification previews' timing in Show Previews—pick Always, When Unlocked, or Never.
* Customize each app's notification style and delivery time.
* Manage Notification Grouping: Automatic, By App, or Off.

**Reference:**

* + 1. https://support.apple.com/guide/iphone/change-notification-settings-iph7c3d96bab/ios
  1. Pg 80 3.2.1.1 Ensure 'Allow screenshots and screen recording' is set to 'Disabled'.

Disabling 'Allow screenshots and screen recording' is important to prevent unauthorized capture of sensitive information, enhancing data security and privacy on the device.

To address this:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Click on the Restrictions tab in the left pane.
* Uncheck the 'Allow screenshots and screen recording' option under the Functionality tab in the right pane.
* Deploy the Configuration Profile.

**References:**

* + 1. https://developer.apple.com/documentation/avfoundation/capture\_setup/requesting\_authorization\_to\_capture\_and\_save\_media
  1. Pg 104 3.2.1.13 Ensure 'Allow trusting new enterprise app authors' is set to 'Disabled'.

Disabling 'Allow trusting new enterprise app authors' is crucial to prevent the installation of potentially unsafe or unauthorized apps, ensuring the security of the device.

To configure:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Navigate to the Restrictions tab on the left.
* Uncheck 'Allow trusting new enterprise app authors' under the Functionality tab on the right.
* Deploy the Configuration Profile.

**Reference:**

* + 1. https://support.apple.com/en-us/HT204460
  1. Pg 131 3.2.1.27 Ensure `Allow password sharing (supervised only) ` is set to `Disabled`.

Disabling 'Allow password sharing (supervised only)' is important to enhance security by preventing the sharing of passwords on supervised devices, reducing the risk of unauthorized access, and maintaining data integrity.

To Configure:

* Launch Apple Configurator.
* Open the Configuration Profile.
* Go to the Restrictions tab on the left.
* Uncheck 'Allow password sharing (supervised only)' under the Functionality tab on the right.
* Deploy the Configuration Profile.

**References:**

* + 1. https://support.apple.com/en-sg/guide/personal-safety/ips3ce9f6e15/web
  1. Pg 142 3.3.1 Ensure 'Managed Safari Web Domains' is `Configured`.

Safari may unknowingly download sensitive files into unsecured app spaces. By setting up specific domains as managed, institutions can ensure a secure container for their data, preventing potential security risks.

To do this in Apple Configurator:

* Open the tool.
* Access the Configuration Profile.
* Click on the Domains tab on the left.
* In the right pane, enter the specific website address(es) under 'Managed Safari Web Domains.'
* Deploy the Configuration Profile.

**References:**

* + 1. https://support.apple.com/en-sg/guide/deployment/depb4c146c2e/web
    2. https://support.apple.com/en-sg/guide/apple-configurator-mac/pmd85719196/2.17/mac/14.0
  1. Pg 156 3.5.1 Ensure 'VPN' is 'Configured.

Configuring a VPN is crucial to enhance security by encrypting data during transmission and utilizing trusted network services, mitigating the risks associated with potential exploitation by malicious users.

To set up the VPN:

Using Apple Configurator:

* Open the tool, Apple Configurator
* Access the Configuration Profile.
* Click on VPN and input the necessary configuration.
* Deploy the Profile.

On the device:

* Navigate to Settings.
* Tap General.
* Select VPN.
* Input the required VPN configuration.

**References:**

* + 1. https://support.apple.com/en-sg/guide/deployment/dep2d2adb35d/web
  1. Pg 168 3.8.1 Ensure 'If Lost, Return to... Message' is 'Configured'.

Setting up a lock screen message is important because it helps honest finders return a lost device by providing contact info, enhancing overall device security.

To configure:

* Launch Apple Configurator.
* Open the Configuration Profile.
* Click on the Lock Screen Message tab on the left.
* In the right pane, enter an appropriate message in the "If Lost, Return to..." field.
* Deploy the Configuration Profile.

References:

* + 1. https://support.apple.com/en-sg/guide/icloud/mmfc0f0165/icloud
  1. Pg 107 3.2.1.15 Ensure 'Allow adding VPN configurations' is set to 'Disabled'.

Setting 'Allow adding VPN configurations' to 'Disabled' is crucial to ensure that only institution-approved VPN setups are used on the device, enhancing network security, and preventing unauthorized configurations.

To prevent users from adding their own VPN configurations:

* Open Apple Configurator.
* Access the Configuration Profile.
* Go to the Restrictions tab on the left.
* In Functionality, uncheck 'Allow adding VPN configurations.'
* Deploy the Configuration Profile.

**References:**

* + 1. https://support.apple.com/guide/deployment/restrictions-for-supervised-devices-dep6b5ae23e9/1/web/1.0
  1. Pg 55 2.4.1 Ensure 'Allow simple value' is set to 'Disabled'.

Configuring 'Allow simple value' to 'Disabled' is important to enhance security by preventing the use of easily guessable or common passwords, reducing the risk of unauthorized access to sensitive information.

To Configure:

* Open Apple Configurator.
* Access the Configuration Profile.
* Click on the Passcode tab on the left.
* Uncheck 'Allow simple value' in the right pane.
* Deploy the Configuration Profile.

**References:**

* + 1. https://support.apple.com/guide/deployment/passcode-payload-settings-dep4d6a472a/web
  1. Pg 57 2.4.2 Ensure 'Minimum passcode length' is set to '6' or greater.

Setting 'Minimum passcode length' to '6' or greater is important to strengthen security by ensuring that users use longer and more complex passcodes. This helps protect the device from unauthorized access, making it more resilient to password guessing or brute-force attacks.

To configure:

* Open Apple Configurator.
* Access the Configuration Profile.
* Click on the Passcode tab on the left.
* Adjust the Minimum passcode length to 6 or more in the right pane.
* Deploy the Configuration Profile.

References:

* + 1. https://support.apple.com/guide/deployment/passcode-payload-settings-dep4d6a472a/web
  1. Pg 69 2.6.1 Ensure 'Allow user to move messages from this account' is set to 'Disabled'.

Message movement, forwarding, and reply is unrestricted by default. It is crucial to disable the option that allows users to move messages from their work email to personal email on their devices. This helps prevent the risk of sensitive information being sent or stored in places that are not secure or managed by the organization.

To configure:

* Launch Apple Configurator.
* Access the Configuration Profile.
* On the left side, click on the Mail tab.
* On the right side, make sure to uncheck the box that says, "Allow user to move messages from this account."

**References:**

* + 1. https://support.apple.com/guide/deployment/mail-payload-settings-dep9c14bfc5/web
  1. Pg 162 3.6.2 Ensure 'Allow Mail Drop' is set to 'Disabled'.

Disabling "Allow Mail Drop" enhances security by preventing large attachments from being sent through external cloud services. Preventing the sharing of sensitive or confidential files through external cloud services.

To Configure:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Click on the Mail tab on the left.
* Uncheck the box next to "Allow Mail Drop" on the right.

**References:**

* + 1. https://support.apple.com/guide/deployment/mail-payload-settings-dep9c14bfc5/web
  1. Pg. 44 2.2.1.12 Ensure 'Show Notification Center in Lock screen' is set to 'Disabled'.

Turning off "Show Notification Center in Lock Screen" is important for privacy. If it's enabled, someone could see your notifications even when the device is locked. Disabling it ensures your information stays private and secure.

To configure:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Navigate to the Restrictions tab on the left.
* On the right, within the Functionality section, deselect the box for "Show Notification Center in Lock Screen."
* Apply the Configuration Profile.

**References:**

* + 1. https://support.apple.com/guide/iphone/control-access-information-lock-screen-iph9a2a69136/14.0/ios/14.0
  1. Pg 22 2.2.1.1 Ensure 'Allow voice dialing while device is locked' is set to 'Disabled.

It's important to disable voice dialing on a locked device to make sure nobody can pretend to be the owner and make calls without permission.

To disable:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Go to the Restrictions tab on the left.
* On the right, in the Functionality section, deselect "Allow voice dialing while device is locked."
* Apply the Configuration Profile.

**References:**

* + 1. Ensure 'Allow voice dialing while device is locked' is set to 'Disabled.
  1. Pg 175 4.3 Ensure 'Automatic Downloads' of 'App Updates' is set to 'Enabled'.

Enabling 'Automatic Downloads' for 'App Updates' is important for security, as it keeps apps up-to-date automatically, reducing the risk of vulnerabilities.

To enable:

* Open Settings.
* Tap iTunes & App Store.
* Turn on Updates under AUTOMATIC DOWNLOADS.

**Reference:**

* + 1. https://support.apple.com/en-us/HT202180
  1. Pg 177 4.4 Ensure 'Find My iPhone/iPad' is set to 'Enabled' on end-user owned devices.

Enabling 'Find My iPhone/iPad' on end-user devices is important because it allows users to locate and secure their device if it's lost or stolen, enhancing the chances of recovery, and preventing unauthorized access to personal information.

To enable:

* Open Settings.
* Tap your name (where Apple ID, iCloud, iTunes & App Store are displayed).
* Tap iCloud.
* Tap Find My iPhone.
* Turn on both Find My iPhone and Send Last Location.

**References:**

* + 1. https://support.apple.com/guide/icloud/set-up-find-my-mmfc0f0c67/icloud
  1. Pg 76 3.1.1 Ensure 'Controls when the profile can be removed' is set to 'Never'.

Setting 'Controls when the profile can be removed' to 'Never' is important to prevent unauthorized removal of essential configuration profiles, ensuring device security and adherence to organizational policies.

To configure:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Click on the General tab on the left.
* On the right, under Security, choose Never for the option 'Controls when the profile can be removed.'
* Apply the Configuration Profile

**References:**

* + 1. https://support.apple.com/guide/deployment/intro-to-mdm-profiles-depc0aadd3fe/web
  1. Pg 137 3.2.2.1 (L1) Ensure 'Force fraud warning' is set to 'Enabled'.

Enabling 'Force fraud warning' is important because it helps protect users by displaying a warning if a website is suspected of fraudulent activity, reducing the risk of falling victim to scams or phishing attempts.

To enable:

* Launch Apple Configurator.
* Access the Configuration Profile.
* Go to the Restrictions tab on the left.
* On the right, under Apps, enable 'Force fraud warning' by checking the box.
* Apply the Configuration Profile.

**References:**

* + 1. https://www.apple.com/legal/privacy/data/en/safari/
    2. https://support.apple.com/guide/deployment/mail-payload-settings-dep9c14bfc5/web

**Cisco IOS 16**

* 1. Pg 208 3.3.4.1 Set 'neighbor password'.

Enabling BGP authentication with a 'neighbor password' is important because it enhances the security of Border Gateway Protocol (BGP) by preventing unauthorized routers from joining.

* To enhance BGP security set up neighbor authentication where possible using the following commands:

hostname(config)#router bgp <<em>bgp\_as-number</em>>

hostname(config-router)#neighbor <<em>bgp\_neighbor-ip</em> | <em>peer-group-name</em>> password <<em>password</em>>

**Reference:**

* + http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\_bgp/command/bgp- n1.html#GUID-A8900842-ECF3-42D3-B188-921BE0EC060B
  + http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\_bgp/command/bgp- m1.html#GUID-159A8006-F0DF-4B82-BB71-C39D2C134205
  1. Pg 173 3.2.2 Set inbound 'ip access-group' on the External Interface.

By default, there is no access group defined. Setting up inbound 'ip access-group' on the External Interface is crucial to stop spoofing attacks and control access. It prevents traffic with incorrect source addresses from the external network, ensuring security by following the least privilege policy.

* To configure use following commands:

hostname(config)#interface {external\_interface}

hostname(config-if)#ip access-group {name | number} in

**References:**

1. http://www.cisco.com/en/US/docs/ios-xml/ios/interface/command/ir- i1.html#GUID-0D6BDFCD-3FBB-4D26-A274-C1221F8592DF
2. http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sec-cr-i1.html#GUID- D9FE7E44-7831-4C64-ACB8-840811A0C993
   1. Pg 163 3.1.1 Set 'no ip source-route'

By default, its enabled. Setting 'no ip source-route' is important to enhance security by preventing the use of source routing, which can be exploited for malicious activities like IP spoofing and unauthorized network access.

* + To Disable source routing enter following code:

hostname(config)#no ip source-route

**References:**

1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr- i4.html#GUID-C7F971DD-358F-4B43-9F3E-244F5D4A3A93
   1. Pg 136 2.2.5 Set 'logging trap informational'

By default, 'logging trap informational' is disabled. Setting 'logging trap informational' is important for managing technology risk by controlling the severity level of logged messages, capturing necessary information without unnecessary details.

* To configure enter the following code:

hostname(config)#logging trap informational

**References:**

1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm\_09.htm l#wp1015177
   1. Pg 128 2.2.1 Set 'logging enable'.

By default, Logging is not enabled. Enabling 'logging enable' is important because it ensures the recording of system activities on Cisco devices. This chronological log serves as a valuable tool for monitoring operational and security-related events, helping manage technology risks effectively.

* To enable enter following commands:

hostname(config)#archive

hostname(config-archive)#log config

hostname(config-archive-log-cfg)#logging enable

hostname(config-archive-log-cfg)#end

**Reference:**

1. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config- mgmt/configuration/xe-16-6/config-mgmt-xe-16-6-book/cm-config-logger.pdf
   1. Pg 58 1.3.2 Set the 'banner-text' for 'banner login'.

No banner is set by default. Setting the 'banner login' is important as it serves legal purposes by obtaining user consent for monitoring, file retrieval, and establishing network administrator authority.

* To configure use the following:

hostname(config)#banner login c

Enter TEXT message. End with the character 'c'. <banner-text>

c

**References:**

1. http://www.cisco.com/en/US/docs/ios- xml/ios/fundamentals/command/A\_through\_B.html#GUID-FF0B6890-85B8-4B6A- 90DD-1B7140C5D22F
   1. Pg 68 1.4.3 Set 'username secret' for all local users.

No passwords are set by default. Setting 'username secret' for local users is important as it enhances security by using MD5-encrypted passwords, preventing unauthorized access. It ensures strong user authentication, especially in situations where centralized authentication services are unavailable.

* To configure use the following:

hostname(config)#username {{em}LOCAL\_USERNAME{/em}} secret {{em}LOCAL\_PASSWORD{/em}}

**References:**

1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/s1/sec-cr-t2- z.html#GUID-5071E577-5249-4EA1-9226-BD426BEAD5B9
   1. Pg 74 1.5.3 Unset 'public' for 'snmp-server community'.

It's important to change 'snmp-server community' from the default 'public' to enhance security. This default is often targeted by unauthorized access attempts, and using a more secure community string helps protect against such threats.

* To disable the default SNMP community string "public" use the following:

hostname(config)#no snmp-server community {public}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr- s2.html#GUID-2F3F13E4-EE81-4590-871D-6AE1043473DE
  1. Pg 122 2.1.6 Set 'service tcp-keepalives-in'.

Disabled by default. Enabling 'service tcp-keepalives-in' is crucial to reduce the risk of unauthorized access. It helps detect and close stale connections, preventing potential misuse and enhancing overall security.

* To enable enter:

hostname(config)#service tcp-keepalives-in

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios- xml/ios/fundamentals/command/R\_through\_setup.html#GUID-1489ABA3-2428- 4A64-B252-296A035DB85E
  1. Pg 130 2.2.2 Set 'buffer size' for 'logging buffered'.

By default, it is disabled. Enabling 'logging buffered' with a specified 'buffer size' is important for effective debugging and monitoring. It allows the device to store log messages internally, aiding in data forensics and technology risk management.

* To Configure buffered logging (with minimum size). Recommended size is 64000 enter the following:

hostname(config)#logging buffered [<em>log\_buffer\_size</em>]

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios/netmgmt/command/reference/nm\_09.htm l#wp1060051
  1. Pg 148 2.3.1.3 Set the 'ntp trusted-key'.

By default, it is disabled. Setting up 'ntp trusted-key' is important because it ensures the authentication of systems for Network Time Protocol (NTP) synchronization. This protects against accidental synchronization with untrusted systems, enhancing overall security.

* To configure use following code:

hostname(config)#ntp trusted-key {ntp\_key\_id}

**References:**

http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr- n1.html#GUID-89CA798D-0F12-4AE8-B382-DE10CBD261DB

* 1. Pg 198 3.3.3.1 Set 'key chain'.

By default, it is not set up. It's important to set up a 'key chain' for RIPv2 routing protocols. This helps enforce strong authentication methods as per security policies, restricting acceptable authentication between network devices.

* To set up:

hostname(config)#key chain {<em>rip\_key-chain\_name</em>}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\_pi/command/iri-cr- a1.html#GUID-A62E89F5-0B8B-4CF0-B4EB-08F2762D88BB
  1. Pg 152 2.3.2 Set 'ip address' for 'ntp server'.

Servers are not configured by default. NTP, or Network Time Protocol, is a system that makes sure all devices on a network have the same accurate time. It helps coordinate events and keeps everything in sync.

* To configure:

hostname(config)#ntp server {ntp-server\_ip\_address}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/bsm/command/bsm-cr- n1.html#GUID-255145EB-D656-43F0-B361-D9CBCC794112
  1. Pg 10 1.1.2 Enable 'aaa authentication login'.

By default, it is disable. Enabling 'aaa authentication login' is important because it brings consistent and centralized control to network access, ensuring secure logins with valid credentials. It also allows emergency access if the AAA server is unavailable, enhancing overall network security.

* To enable enter following command:

hostname(config)#aaa authentication login {default | aaa\_list\_name} [passwd- expiry] [method1] [method2]

**Reference:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sec-cr-a1.html#GUID- 3DB1CC8A-4A98-400B-A906-C42F265C7EA2
  1. Pg 53 1.2.12 Set 'exec-timeout' to less than or equal to 10 min on 'ip http'.

By default, it is disable. Setting 'exec-timeout' to less than or equal to 10 minutes on 'ip http' is important to prevent unauthorized users from misusing abandoned sessions, enhancing security. It ensures that if no input is detected within the specified interval, the session is disconnected, reducing the risk of unauthorized access.

* To enable:

ip http timeout-policy idle 600 life {nnnn} requests {nn}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios- xml/ios/fundamentals/command/D\_through\_E.html#GUID-76805E6F-9E89-4457- A9DC-5944C8FE5419
  1. Pg 88 1.5.10 Require 'aes 128' as minimum for 'snmp-server user' when using SNMPv3.

SNMP username as not set by default. Requiring 'aes 128' as a minimum for 'snmp-server user' in SNMPv3 is crucial because it significantly reduces the risk of unauthorized access by ensuring robust encryption of messages in transit.

* To configure:

For each SNMPv3 user created on your router add privacy options by issuing the following command:

hostname(config)#snmp-server user {user\_name} {group\_name} v3 auth sha {auth\_password} priv aes 128 {priv\_password} {acl\_name\_or\_number}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/snmp/command/nm-snmp-cr- s5.html#GUID-4EED4031-E723-4B84-9BBF-610C3CF60E31
  1. Pg 102 2.1.1.1.1 Set the 'hostname'.

The default hostname is Router. Setting the 'hostname' is essential for SSH setup, impacting prompts and default configuration filenames. Organizations need to plan and assign a suitable hostname for each router in the enterprise network.

* To configure an appropriate host name for the router:

hostname(config)#hostname {<em>router\_name</em>}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios- xml/ios/fundamentals/command/F\_through\_K.html#GUID-F3349988-EC16-484A- BE81-4C40110E6625
  1. Pg 96 1.6.3 Configuring Kerberos.

By default, Kerberos is not set up. Setting up Kerberos is important for secure user and service authentication on the network. It simplifies the login process, and in Cisco IOS XE, it adds extra security for services like Telnet and others, requiring users to authenticate both to the router and the Key Distribution Center.

To configure:

* Add users to the KDC database using:

Hostname# ank {username@REALM}

Hostname# ank {username/instance@REALM}

* Create SRVTABs on the KDC for network services on Kerberized hosts:

Execute: Hostname# ark {SERVICE/HOSTNAME@REALM}

* Define a Kerberos Realm:

Set the local realm: Hostname#(config)kerberos local-realm {kerberos-realm}

Configure the Kerberos server: Hostname#(config)kerberos server {kerberos-realm {hostname | ip-address}} {port-number}

Specify the realm: Hostname#(config)kerberos realm {dns-domain | host} {kerberos-realm}

**References:**

* + 1. https://www.cisco.com/c/en/us/td/docs/ios- xml/ios/sec\_usr\_cfg/configuration/xe-16-5/sec-usr-cfg-xe-16-5-book/sec-cfg- kerberos.html
  1. Pg 104 2.1.1.1.2 Set the 'ip domain-name'.

By default, no domain is set. Setting the 'ip domain-name' is important because it establishes a default domain name for the router, helping complete unqualified hostnames and enabling SSH. Organizations need to plan and choose a suitable domain name for their network.

* To configure use following:

hostname (config)#ip domain-name {<em>domain-name</em>}

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr/command/ipaddr- i3.html#GUID-A706D62B-9170-45CE-A2C2-7B2052BE2CAB
  1. Pg 124 2.1.7 Set 'service tcp-keepalives-out'.

It is disabled by default. Turning on 'service tcp-keepalives-out' is crucial. It generates keepalive packets for idle outgoing connections, preventing security risks associated with stale connections. This helps detect and close failed connections, contributing to a safer network.

* To enable type:

hostname(config)#service tcp-keepalives-out

**References:**

* + 1. http://www.cisco.com/en/US/docs/ios- xml/ios/fundamentals/command/R\_through\_setup.html#GUID-9321ECDC-6284- 4BF6-BA4A-9CEEF5F993E5

**Microsoft Windows 10 Enterprise**

* + 1. Pg 889 18.9.12.1 Ensure 'Allow Use of Camera' is set to 'Disabled'.

In high-security setups, it's important to turn off camera usage to prevent privacy breaches and data leaks. Cameras, if left enabled, could be misused for unauthorized surveillance, or capturing sensitive information, posing serious security threats. Setting 'Allow Use of Camera' to 'Disabled' is a proactive measure to reduce these risks and enhance overall security. By default, it is enabled.

* Using Group Policy, set the UI path mentioned below to 'Disabled':

Computer Configuration\Policies\Administrative Templates\Windows Components\Camera\Allow Use of Camera.

**References:**

* + - 1. https://learn.microsoft.com/en-us/answers/questions/312293/group-policy-windows-10-allow-access-to-the-camera
    1. Pg 811 18.9.11.2.3 Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled'.

By default, it is disabled. Enabling this setting is crucial to make sure that if a user loses their main way of accessing an encrypted OS volume or if the system fails its boot checks, the recovery key can be used for system recovery. This helps avoid data loss and ensures access to the encrypted volume.

* Using Group Policy, following UI path:

Computer Configuration\Policies\Administrative Templates\Windows

Components\BitLocker Drive Encryption\Operating System Drives\Choose how BitLocker-protected operating system drives can be recovered.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/configure?tabs=common
    1. Pg 673 18.8.22.1.9 Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'.

Ensuring 'Turn off Search Companion content file updates' is set to 'Enabled' prevents Search Companion from automatically downloading content updates during searches, reducing the risk of revealing sensitive information. By default, it is disabled.

* Using Group Policy, following UI path:

Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates.

**References:**

1. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-vdi-recommendations-2004

* + 1. Pg 572 18.5.10.2 Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'.

Ensuring 'Turn off Search Companion content file updates' is set to 'Enabled' prevents Search Companion from automatically downloading content updates during searches, reducing the risk of inadvertently revealing sensitive information. The impact is that Search Companion does not fetch content updates during searches. By default, it is disabled.

* Using Group Policy, following UI path:

Computer Configuration\Policies\Administrative Templates\Network\Microsoft

Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking Services

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/win32/p2psdk/what-is-peer-networking-
    1. Pg 540 18.4.4 Ensure 'MSS: (DisableSavePassword) Prevent the dial -up password from being saved' is set to 'Enabled'.

By default, it is disabled. Enabling 'Prevent the dial-up password from being saved' is important to stop attackers from easily accessing the organization's network if they steal a user's computer with saved passwords.

* Using Group Policy, following UI path:

Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS:(DisableSavePassword) Prevent the dial-up password from being saved.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication
    1. Pg 505 18.2.1 Ensure LAPS AdmPwd GPO Extension / CSE is installed.

By default, it is not installed. Installing the LAPS tool is crucial for enhancing security by automatically setting unique local Administrator passwords on domain-attached workstations and servers. This prevents attackers from easily compromising multiple systems if one local Administrator password is exposed.

* To use LAPS:

Make an update to the Active Directory Schema and install the Group Policy Client Side Extension (CSE) on each managed computer.

Ensure the file AdmPwd.dll is located at C:\Program Files\LAPS\CSE\AdmPwd.dll and registered in Windows.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview
    1. Pg 207 2.3.8.1 Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'.

By default, it is disabled. Enabling 'Microsoft network client: Digitally sign communications (always)' ensures that SMB packets are signed, preventing attackers on the same network from interrupting, ending, or stealing sessions. This helps authenticate users and servers, preventing unauthorized access and data manipulation.

* To configure using Group Policy, following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local

Policies\Security Options\Microsoft network client: Digitally sign communications (always)

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always
    1. Pg 759 18.9.6.2 Ensure 'Block launching Universal Windows apps with Windows Runtime API access from hosted content.' is set to 'Enabled'.

By default, it is disabled. Enabling 'Block launching Universal Windows apps with Windows Runtime API access from hosted content' prevents potentially malicious apps from being run directly from web content, enhancing system security. This helps ensure that only approved applications are installed, reducing the risk of unauthorized or harmful software.

o To configure using Group Policy, following UI path: Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Block launching Universal Windows apps with Windows Runtime API access from hosted content.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/client-management/mdm/policy-csp-admx-appxruntime
    1. Pg 433 9.3.8 Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'.

By default, it is set at 4096 KB. Setting the 'Windows Firewall: Public: Logging: Size limit ' to '16,384 KB or greater' ensures that Windows Firewall logs have sufficient space to record events. This helps in diagnosing system issues or identifying unauthorized activities by maintaining an adequate log size, preventing crucial information from being overwritten too quickly.

* To configure enter the following UI path to 16,384 KB or greater:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced

Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB)

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure-logging?tabs=intune
    1. Pg 371 5.37 Ensure 'Windows Push Notifications System Service (WpnService)' is set to 'Disabled'.

The default value is automatic. Disabling the 'Windows Push Notifications System Service (WpnService)' is important in high-security environments to prevent external systems from impacting secure workstations through 3rd-party notifications and updates from the cloud/Internet.

* To establish the recommended configuration via GP, set the following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Windows Push Notifications System Service

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/apps/design/shell/tiles-and-notifications/windows-push-notification-services--wns--overview
    1. Pg 357 5.30 Ensure 'SSDP Discovery (SSDPSRV)' is set to 'Disabled'.

The default setting is manual. Turning off the 'SSDP Discovery (SSDPSRV)' service is important because it stops devices from automatically connecting to and discovering networked services. This helps to lower the security risk associated with Universal Plug and Play (UPnP) in a security-focused environment.

* To turn off configuration via GP, set the following UI path to disabled:

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\SSDP Discovery

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/win32/upnp/overview-of-universal-plug-and-play
    1. Pg 598 18.5.23.2.1 Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disabled'.

By default, it is enabled. Disabling 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' prevents Windows from automatically connecting to unknown networks, enhancing security by avoiding potentially unsafe or unauthorized connections.

* To configure via GP, set the following UI path to disabled:

Computer Configuration\Policies\Administrative Templates\Network\WLAN Service\WLAN Settings\Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services.

**References:**

* + - 1. https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/configure-wifi-sense-and-paid-wifi-service
    1. Pg 216 2.3.9.2 Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'.

By default, it is disabled. Enabling this setting enhances security by requiring packet signing for the SMB server, preventing attackers from hijacking sessions and gaining unauthorized access to data on the network.

* To configure via GP, set the following UI path to enabled:

Computer Configuration\Policies\Windows Settings\Security Settings\Local

Policies\Security Options\Microsoft network server: Digitally sign communications (always)

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always
    1. Pg 67 1.2.2 Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'.

By default, it is set to 0 failed logon attempts. It's crucial to set an account lockout threshold to boost security and prevent online password attacks. Keeping the threshold low helps balance security and usability, minimizing accidental lockouts. However, setting it to 0 poses a risk of undetected attacks, emphasizing the need for a well-configured threshold.

* To configure via GP, set the following UI path to 10 or fewer invalid login attempts, but not 0:

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold
    1. Pg 172 2.3.4.2 Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'.

By default, it is disabled, meaning that any user can install a printer drive as part of connecting to a shared printer. Preventing users from installing printer drivers is crucial for maintaining security in a high-risk environment. Allowing only administrators to perform this action.

* To enable configuration via GP, set the following UI path:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-prevent-users-from-installing-printer-drivers
    1. Pg 189 2.3.7.2 Ensure 'Interactive logon: Don't display last signed-in' is set to 'Enabled'.

Enabling "Interactive logon: Don't display last signed-in" is important to prevent potential attackers from visually collecting account names of the last users who logged in. By default, it is disabled.

* To configure via GP, set the following UI path to Enabled:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Don't display last signed-in

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name
    1. Pg 254 2.3.11.1 Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'.

Enabling this setting helps Windows systems communicate securely by allowing Local System services to use the computer identity for certain types of authentications, ensuring proper data protection. By default, it is disabled.

* To configure via GP, set the following UI path to Enabled:

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-local-system-to-use-computer-identity-for-ntlm
    1. Pg 716 18.8.34.6.2 Ensure 'Allow network connectivity during connected- standby (plugged in)' is set to 'Disabled'.

It is enabled by default. Disabling this setting is important because it prevents potential unauthorized access to the computer over a WLAN network while it's unattended, plugged in, and in a sleep state, enhancing security.

* To configure via GP, set the following UI path to Disabled:

Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in).

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/modern-standby-network-connectivity
    1. Pg 337 5.20 Ensure 'Remote Desktop Configuration (SessionEnv)' is set to 'Disabled'.

The default setting is set to manual. Disabling 'Remote Desktop Configuration (SessionEnv)' is important in high-security environments because it reduces the security risk associated with Remote Desktop access. This measure ensures that only local console access is permitted, enhancing overall security. it's important to note that users will be unable to use Remote Assistance with this setting disabled.

o To configure via GP, set the following UI path to Disabled:

Computer Configuration\Policies\Windows Settings\Security Settings\System Services\Remote Desktop Configuration

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access
    1. Pg 399 9.1.7 Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'.

By default, it is set to ‘No’. Setting up Logging dropped packets to ‘Yes’ is crucial because it helps identify and troubleshoot system problems, uncover unauthorized activities, and improves security by providing a record of why and when inbound packets were discarded. Without these logs, determining the root cause of issues or malicious activities becomes difficult or even impossible.

* To configure via GP, set the following UI path to ‘Yes’:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets.

**References:**

* + - 1. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure-logging?tabs=intune

**Red Hat Enterprise Linux 8**

* 1. Pg 76 1.2.2 Disable the rhnsd Daemon.

Disabling the rhnsd daemon is important because it prevents automatic actions based on patches from being executed without appropriate consideration. This is crucial for organizations that follow patch management policies, allowing them to test the impact of patches before deploying them in a production environment.

* Run the following command to disable rhnsd:

# systemctl --now disable rhnsd

**References:**

* + - 1. https://access.redhat.com/documentation/id-id/red\_hat\_network/5.0.0/html/reference\_guide/s1-rhnsd-disable
    1. Pg 435 5.2.17 Ensure SSH AllowTcpForwarding is disabled.

Disabling SSH AllowTcpForwarding is important because leaving port forwarding enabled can expose the organization to security risks and potential backdoors.

* To configure edit the /etc/ssh/sshd\_config file to set the parameter as follows:

AllowTcpForwarding no

**References:**

* + - 1. 1. https://www.ssh.com/ssh/tunneling/example
    1. Pg 69 1.1.22 Disable Automounting.

Disabling automounting is important because it prevents unauthorized access to device contents by individuals with physical access. With automounting enabled, anyone can attach a USB drive or disc, making its contents available even without proper permissions.

* Enter the following command to disable autofs:

# systemctl --now disable autofs

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/storage\_administration\_guide/nfs-autofs
    1. Pg 64 1.1.19 Ensure nosuid option set on removable media partitions.

Setting the nosuid option on removable media partitions is important because it prevents users from introducing privileged programs onto the system.

* To configure edit the /etc/fstab file and add nosuid to the fourth field (mounting options) of all removable media partitions.

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/managing\_file\_systems/mounting-nfs-shares\_managing-file-systems
    1. Pg 143 1.9 Ensure updates, patches, and additional security software are installed.

Regularly updating your software, applying patches, and adding security tools is crucial. It helps fix security issues, adds new features, and overall boosts your system's safety.

* The following command will install all available updates:

# dnf update

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/security\_guide/chap-keeping\_your\_system\_up-to-date
    1. Pg 377 4.3 Ensure logrotate is configured.

Configuring logrotate is important because it helps manage log files effectively by rotating them regularly. This prevents logs from filling up the system and becoming unmanageably large.

* To configure edit: /etc/logrotate.conf and /etc/logrotate.d/\* to ensure logs are rotated according to site policy

**References:**

* + - 1. https://www.redhat.com/sysadmin/setting-logrotate
    1. Pg 74 1.2.1 Ensure Red Hat Subscription Manager connection is configured.

Configuring the Red Hat Subscription Manager connection is crucial for systems to receive regular patch updates.

* Run the following command to connect to the Red Hat Subscription Manager:

# subscription-manager register

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/configuring\_basic\_system\_settings/assembly\_registering-the-system-and-managing-subscriptions\_configuring-basic-system-settings
    1. Pg 155 2.2.1.1 Ensure time synchronization is in use.

Time synchronization is important for supporting time-sensitive security mechanisms like Kerberos and ensuring consistent time records in log files. It aids in forensic investigations and promotes a standardized time across the enterprise.

* Run the following command to install chrony:

# dnf install chrony

**Refrences:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/system\_administrators\_guide/ch-configuring\_ntp\_using\_the\_chrony\_suite
    1. Pg 297 3.6 Disable IPv6.

Disabling IPv6 is important to reduce the attack surface of the system if IPv6 or dual-stack configurations are not implemented or intended for use.

* To disable IPv6 through the GRUB2 config:

Edit /etc/default/grub and add ipv6.disable=1

to the GRUB\_CMDLINE\_LINUX parameters:

GRUB\_CMDLINE\_LINUX="ipv6.disable=1"

Run the following command to update the grub2 configuration:

# grub2-mkconfig –o /boot/grub2/grub.cfg

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/configuring\_and\_managing\_networking/using-networkmanager-to-disable-ipv6-for-a-specific-connection\_configuring-and-managing-networking#doc-wrapper
    1. Pg 66 1.1.20 Ensure noexec option set on removable media partitions.

Setting the noexec option on removable media partitions is important because it prevents users from executing programs directly from the removable media.

* To configure:

edit the /etc/fstab file and add noexec to the fourth field (mounting options) of all removable media partitions.

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/managing\_file\_systems/mounting-file-systems\_managing-file-systems#doc-wrapper
    1. Pg 266 3.4.3.6 Ensure nftables default deny firewall policy.

It is set as default to accept. Setting nftables to deny enhances security by blocking unspecified packets, making it easier to allow only desired traffic.\

* To configure run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

# nft chain <table family> <table name> <chain name> { policy drop \; }

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/configuring\_and\_managing\_networking/getting-started-with-nftables\_configuring-and-managing-networking
    1. Pg 274 3.4.4.1.1 Ensure iptables default deny firewall policy.

Having a default deny all policy in iptables ensures that any network activity not explicitly configured will be rejected. This is important because, with a default accept policy, the firewall would accept any packet not configured to be denied.

* To implement a default DROP policy:

# iptables -P INPUT DROP

# iptables -P OUTPUT DROP

# iptables -P FORWARD DROP

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/security\_guide/sec-setting\_and\_controlling\_ip\_sets\_using\_iptables
    1. Pg 431 5.2.15 Ensure SSH warning banner is configured.

Having an SSH warning banner is important because it warns users about the site's connection policies. This message, shown before login, can help prosecute trespassers by making the rules and policies clear.

* To configure Edit the /etc/ssh/sshd\_config file to set the parameter as follows:

Banner /etc/issue.net

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_openstack\_platform/13/html/security\_and\_hardening\_guide/using\_director\_to\_configure\_security\_hardening#use-ssh-banner-text\_using-director-to-configure-security-hardening
    1. Pg 426 5.2.13 Ensure SSH Idle Timeout Interval is configured.

Configuring the SSH Idle Timeout Interval is important to prevent unauthorized access in cases where a user leaves their computer unattended without locking the screen. Setting a timeout reduces this risk by disconnecting inactive sessions.

The default value is : ClientAliveInterval 0 and ClientAliveCountMax 3

* To configure edit the /etc/ssh/sshd\_config file to set the parameters according to best practices. This should include ClientAliveInterval between 1 and 900 and ClientAliveCountMax of 0:

ClientAliveInterval 900

ClientAliveCountMax 0

**References:**

* + - 1. https://man.openbsd.org/sshd\_config
    1. Pg 147 1.11 Ensure system-wide crypto policy is FUTURE or FIPS.

Choosing a crypto policy for your system is important. If you need compatibility with older, less secure protocols, you might go for LEGACY. But for better security, FUTURE or FIPS are recommended. They protect against vulnerabilities and work well with modern cryptographic protocols. The policy levels are: (DEFAULT, LEGACY, FUTURE, and FIPS) The default setting is set to ‘Default’

* To configure run the following command to change the system-wide crypto policy:

# update-crypto-policies --set FUTURE

OR

* To switch the system to FIPS mode, run the following command:

# fips-mode-setup –enable

**References:**

* + - 1. https://access.redhat.com/articles/3642912#what-polices-are-provided-1
      2. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/8/html/security\_hardening/using-the-system-wide-cryptographic-policies\_security-hardening
    1. Pg 23 1.1.1.2 Ensure mounting of vFAT filesystems is limited.

Limiting the use of vFAT filesystems makes your system more secure. However, keep in mind that disabling vFAT support may impact your ability to transfer files using USB sticks and could prevent some systems from booting.

* To configure edit or create a file in the /etc/modprobe.d/ directory ending in .conf. (For example: vim /etc/modprobe.d/vfat.conf):

install vfat /bin/true

* To configure run the following command to unload the vfat module:

# rmmod vfat

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/storage\_administration\_guide/sect-using\_the\_mount\_command-mounting
    1. Pg 78 1.2.3 Ensure GPG keys are configured.

Configuring GPG keys is important because most package managers use GPG key signing to verify the integrity of packages during installation. This ensures that updates come from a valid and trusted source, protecting against the risk of spoofing.

* To configure update your package manager GPG keys in accordance with site policy.

**References:**

* + - 1. https://www.redhat.com/sysadmin/rpm-gpg-verify-packages
    1. Pg 82 1.2.5 Ensure package manager repositories are configured.

Configuring package manager repositories is important because it ensures that systems receive the latest patches and updates.

* To Configure make sure your package manager repositories are set according to site policy.

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/security\_guide/chap-keeping\_your\_system\_up-to-date
      2. https://www.redhat.com/sysadmin/how-manage-packages
    1. Pg 249 3.4.2.5 Ensure network interfaces are assigned to appropriate zone.

Assigning network interfaces to appropriate zones is important because firewall zones define the trust level of network connections or interfaces. If a network interface is not assigned to the correct zone, it may allow unexpected or undesired network traffic.

* To configure run the following command to assign an interface to the approprate zone.

# firewall-cmd --zone=<Zone NAME> --change-interface=<INTERFACE NAME>

(Example: # firewall-cmd --zone=customezone --change-interface=eth0)

**References:**

* + - 1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/security\_guide/sec-working\_with\_zones

20. Pg 264 3.4.3.5 Ensure nftables outbound and established connections are configured.

Configuring nftables for outbound and established connections is important because without proper rules in place, the default policy may drop all packets. This could lead to the prevention of network usage.

* To Configure nftables. The following commands will implement a policy to allow all outbound connections and all established connections:

# nft add rule inet filter input ip protocol tcp ct state established accept

# nft add rule inet filter input ip protocol udp ct state established accept

# nft add rule inet filter input ip protocol icmp ct state established accept

# nft add rule inet filter output ip protocol tcp ct state new,related,established accept

# nft add rule inet filter output ip protocol udp ct state new,related,established accept

# nft add rule inet filter output ip protocol icmp ct state new,related,established accept

**References:**

1. https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/security\_guide/sec-creating\_and\_managing\_nftables\_tables\_chains\_and\_rules

**SUSE Linux Enterprise 15**

1. Pg 242 3.5.2.8 Ensure default deny firewall policy.

By default, it is set to accept. Setting a default deny firewall policy is crucial because it enhances security by blocking all incoming traffic unless specifically allowed. This approach, known as whitelisting, makes it easier to manage and ensures that only approved activities are permitted.

* To configure run the following command for the base chains with the input, forward, and output hooks to implement a default DROP policy:

# nft chain <table family> <table name> <chain name> { policy drop \; }

**References:**

1. https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-security-firewall.html

1. Pg 381 5.2.7 Ensure SSH MaxAuthTries is set to 4 or less.

By default, it is set to 6. It's important to set SSH MaxAuthTries to 4 or less to reduce the risk of successful brute force attacks on the server. This parameter limits the number of authentication attempts per connection.

* To configure edit the /etc/ssh/sshd\_config file to set the parameter as follows:

MaxAuthTries 4

**References:**

1. https://documentation.suse.com/sled/15-SP5/html/SLED-all/cha-ssh.html

1. Pg 402 5.2.20 Ensure SSH AllowTcpForwarding is disabled.

By default, it is enabled. Disabling SSH AllowTcpForwarding is crucial because it prevents potential security risks and backdoors. When enabled, port forwarding in SSH could be exploited by cybercriminals or malware to hide unauthorized communications and exfiltrate sensitive data from the network.

* To configure edit the /etc/ssh/sshd\_config file to set the parameter as follows:

AllowTcpForwarding no

**References:**

1. https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-ssh.html

1. Pg 59 1.1.20 Ensure nodev option set on removable media partitions.

It's important to ensure the "nodev" option is set on removable media partitions to prevent security risks. This option prohibits the filesystem on removable media from containing special devices.

* To configure edit the /etc/fstab file and add nodev to the fourth field (mounting options) of all removable media partitions. Mount points that contain words such as floppy or cdrom.

**References:**

1. https://www.suse.com/support/kb/doc/?id=000020660

1. Pg 347 4.2.4 Ensure logrotate is configured.

Ensuring logrotate is configured is important because it helps manage log files, preventing them from filling up the system and becoming unmanageable. Regular log rotation makes files smaller and more manageable.

* To configure edit /etc/logrotate.conf and /etc/logrotate.d/\* to ensure logs are rotated according to site policy.

**References:**

1. https://documentation.suse.com/sles/15-SP3/html/SLES-all/cha-tuning-syslog.html

1. Pg 132 2.2.1.2 Ensure systemd-timesyncd is configured.

It's important to configure systemd-timesyncd because it helps synchronize the system clock across the network. This ensures accurate timekeeping, which is crucial for various system operations and helps maintain consistency across networked systems.

* To configure edit the file /etc/systemd/timesyncd.conf and add/modify the following lines:

NTP=0.suse.pool.ntp.org 1.suse.pool.ntp.org #Servers listed should be In Accordance With Local Policy

FallbackNTP=2.suse.pool.ntp.org 3.suse.pool.ntp.org #Servers listed should be

In Accordance With Local Policy

RootDistanceMax=1 #should be In Accordance With Local Policy

* Run the following commands to enable and start systemd-timesyncd:

# systemctl --now enable systemd-timesyncd.service # timedatectl set-ntp true

**References:**

1. https://manpages.opensuse.org/Tumbleweed/systemd/systemd-time-wait-sync.service.8.en.html

1. Pg 175 3.1.1 Disable IPv6.

Disabling IPv6 is recommended to enhance security by reducing the ways in which the system can be attacked. If your organization does not use or require IPv6, turning it off helps simplify and secure your network configuration. This is because unused services and protocols can potentially introduce security risks.

* To configure IPv6 through sysctl settings:

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/\* file:

net.ipv6.conf.all.disable\_ipv6 = 1 net.ipv6.conf.default.disable\_ipv6 = 1

* Run the following commands to set the active kernel parameters:

# sysctl -w net.ipv6.conf.all.disable\_ipv6=1

# sysctl -w net.ipv6.conf.default.disable\_ipv6=1 # sysctl -w net.ipv6.route.flush=1

**References:**

1. https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-network.html?\_gl=1\*m9brsb\*\_ga\*ODMzNjk2ODkwLjE2OTYxMDMyNDY.\*\_ga\_JEVBS2XFKK\*MTcwMTA5MzI4Ni4yLjEuMTcwMTA5NzM1Ny42MC4wLjA.#sec-network-ipv6-config

1. Pg 178 3.1.2 Ensure wireless interfaces are disabled.

Turning off wireless interfaces when not in use is important for security. If you're not using Wi-Fi, keeping it disabled helps protect your system from potential security threats.

* To configure run the following command to disable any wireless interfaces:

# ip link set <interface> down

**References:**

1. https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-nm.html

1. Pg 333 4.2.1.4 Ensure logging is configured.

Configuring logging is important because it enables the capture of crucial security-related information, such as successful and failed login attempts, root login attempts, and more.

* To configure edit the following lines in the /etc/rsyslog.conf and /etc/rsyslog.d/\*.conf files as appropriate for your environment
* Run the following command to reload the rsyslogd configuration:

# systemctl restart rsyslog

**References:**

1. https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-tuning-syslog.html

1. Pg 269 3.5.3.3.4 Ensure IPv6 firewall rules exist for all open ports.

It's important to have IPv6 firewall rules for all open ports because, without them, the default firewall policy would drop all packets to these ports. Firewall rules act as a security measure to control and regulate incoming and outgoing network traffic.

* For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:

# ip6tables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

**References:**

1. https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-security-firewall.html

1. Pg 58 1.1.19 Ensure noexec option set on removable media partitions.

Setting the "noexec" option on removable media partitions is important because it prevents users from executing programs directly from the removable media. This helps enhance security by reducing the risk of introducing potentially malicious software onto the system through executable binaries on external devices.

* To configure edit the /etc/fstab file and add noexec to the fourth field (mounting options) of all removable media partitions.

**References:**

1. https://www.suse.com/support/kb/doc/?id=000020660

1. Pg 405 5.2.22 Ensure SSH MaxSessions is limited.

Limiting the MaxSessions parameter is important to protect the system from denial of service caused by too many concurrent sessions. By default, it is set at 10 (It is still acceptable as long as it’s below 10). For better results set it at 5 or below.

* To configure edit the /etc/ssh/sshd\_config file to set the parameter as follows:

MaxSessions 5

**References:**

1. https://documentation.suse.com/suma/4.3/en/suse-manager/client-configuration/contact-methods-saltssh.html

1. Pg 67 1.2.2 Ensure package manager repositories are configured.

Configuring package manager repositories is important to ensure that systems receive the latest patches and updates. Misconfigured repositories may lead to the system not identifying important patches or the introduction of compromised software from a rogue repository.

* Configure your package manager repositories according to site policy.

**References:**

1. https://documentation.suse.com/suma/4.2/en/suse-manager/client-configuration/repositories.html

1. Pg 66 1.2.1 Ensure GPG keys are configured.

Configuring GPG keys is important because package managers use GPG key signing to verify/check the integrity of packages during installation. This ensures that updates come from a valid and trusted source, protecting the system against spoofing, and preventing the installation of malware.

* To configure update your package manager GPG keys in accordance with site policy.

**References:**

1. https://documentation.suse.com/suma/4.2/en/suse-manager/client-configuration/gpg-keys.html

15. Pg 130 2.2.1.1 Ensure time synchronization is in use.

Time synchronization is vital for security mechanisms like Kerberos and ensures consistent time records in log files for effective forensic investigations.

* To configure on systems where host based time synchronization is not available install chrony OR enable systemd-timesyncd:
* Run the following command to install chrony:

# zypper install chrony

OR

* Run the following command to enable systemd-timesyncd

# systemctl enable systemd-timesyncd

**References:**

1. https://manpages.opensuse.org/Tumbleweed/systemd/systemd-time-wait-sync.service.8.en.html

16. Pg 171 2.4 Ensure nonessential services are removed or masked.

It is important to review and, if not required, stop, or remove nonessential services and mask them if necessary to minimize the potential risk and attack vectors posed by open ports. This helps reduce the system's attack surface and enhances security.

* To configure run the following command to remove the package containing the service:

# zypper remove <package\_name>

Or

* If required packages have a dependency run the following command to stop and mask the service:

# systemctl --now mask <service\_name>

**References:**

1. https://documentation.suse.com/smart/systems-management/pdf/reference-systemctl-enable-disable-services\_draft\_en.pdf

17. Pg 232 3.5.2.3 Ensure iptables are flushed.

Flushing iptables rules is important to ensure simplicity and reduce complexity in the use of nftables, the replacement for iptables. Mixing iptables and nftables increases the chance of errors, so flushing iptables helps maintain a clean and manageable firewall configuration.

* To configure Remediation run the following commands to flush iptables: For iptables:

# iptables -F

* For ip6tables

# ip6tables -F

**References:**

1. https://www.suse.com/c/simple-firewall-configuration-using-netfilteriptables/

18. Pg 74 1.3.3 Ensure sudo log file exists.

Having a sudo log file is important because it provides an audit trail for sudo commands, aiding in security monitoring, compliance with standards, and troubleshooting.

* To configure edit the file /etc/sudoers or a file in /etc/sudoers.d/ with visudo or visudo -f <PATH TO FILE> and add the following line:

Defaults logfile="<PATH TO CUSTOM LOG FILE>"

* Example:

Defaults logfile="/var/log/sudo.log"

**References:**

1. https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-adm-sudo.html

19. Pg 118 1.9 Ensure updates, patches, and additional security software are installed.

It is important to install updates, patches, and additional security software regularly to address security vulnerabilities, enhance functionality, and ensure the system's overall security posture.

* Use your package manager to update all packages on the system according to the site policy. To install all available updates, enter the following command:

# zypper update

**References:**

1. https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-sw-cl.html

20. Pg 223 3.5.1.6 Ensure unnecessary services and ports are not accepted.

It is crucial to block unnecessary services and ports to minimize the system's attack surface. In essence, restricting access to only essential services and ports helps enhance overall security by reducing potential entry points for attackers.

* To configure run the following command to remove an unnecessary service:

# firewall-cmd --remove-service=<service>

* Example:

#firewall-cmd --remove-service=cockpit

* Run the following command to remove an unnecessary port:

# firewall-cmd --remove-port=<port-number>/<port-type>

* Example:

# firewall-cmd --remove-port=25/tcp

* Run the following command to make new settings persistent:

# firewall-cmd --runtime-to-permanent

**References:**

1. https://access.redhat.com/documentation/en-

us/red\_hat\_enterprise\_linux/8/html/securing\_networks/using-and-configuring- firewalls\_securing-networks

2. https://documentation.suse.com/sles/15-SP2/html/SLES-all/cha-security-firewall.html