In the NetApp Data ONTAP storage cluster's SSH security configuration, both weak and strong Ciphers, Key Exchange Algorithms, and MAC Algorithms are active.

- Why should we remove weak Ciphers, Key Exchange Algorithms, and MAC Algorithms from the storage clusters and associated end devices?

Summary:

Remove weak ciphers, key exchange algorithms, and MAC algorithms from NetApp storage clusters and associated end devices.

In-depth:

In NetApp storage clusters, both weak and strong Ciphers, Key Exchange Algorithms, and MAC Algorithms are active. It is best advised and recommended to allow/ keep strong ciphers, key exchange algorithms, and MAC algorithms only for SSH connections. And remove weak ones from cluster SSH security configurations due to SSH high-security connections and be followed across all the other the infrastructure devices like OS, network, servers (physical and virtual), and storage.

- If weak ones are active in cluster SSH configuration, it is also red alerted while having a security scan of the storage system configurations.
- If the end devices using weak ones, then engineers need to upgrade the application/ system configuration and involve the respective vendor for their 2nd opinion to understand any dependency.
- If none of the end devices in the infrastructure using weak ones like "3des-cbc", "aes128-cbc", "aes192- cbc", "hmac-sha1-96", "hmac-sha1" "SHA-1", "diffie-hellman-group-exchange-sha1", "diffie-hellman-group14-sha1", "hmac-md5" … Then remove them from SSH security configurations.
- It will maintain SSH connection compliance and security.
- Follow the right design and recommendations in storage arrays. The client's storage infrastructure be better optimized.

Reason(s) for the activity:

- In the long run, it is helpful for high SSH security accessibility.
- Security of business data/ connection is of utmost importance even though there requires minute modification in configuration.

Perform removal of weak ones from storage clusters like below:

Step 1: Check for SSH configurations:

```
cluster_name::> security ssh show
```

Step 2: Remove weak "Ciphers", or, "Key Exchange Algorithms", or, "MAC Algorithms":

```
cluster_name::> security ssh remove -vserver vserver_name -ciphers cipher_name
cluster_name::> security ssh remove -vserver vserver_name -mac-algorithms mac-algorithms_name
cluster_name::> security ssh remove -vserver vserver_name -key-exchange-algorithms key-exchange-algorithms_name
```

Step 3: Validate the SSH configurations:

```
cluster_name::> security ssh show
```

NetApp's feedback:

- They advised checking with application/ system/ end-device dependency and are not disabling/ removing them by default if in infrastructure running any old/ legacy application/ device. If all the devices are running the latest and up-to-date, perform this task manually.
- Or engage the NetApp account team, specific to the customer, as per requirement.

Where,

Abbreviation	Details
Data ONTAP/ ONTAP	The operating system of NetApp AFF/FAS array models [ONTAP or Data ONTAP or Clustered Data ONTAP (cDOT) or Data ONTAP 7-Mode is NetApp's proprietary operating system].
NetApp	Storage vendor.
MAC	Message Authentication Code
CBC	Cipher Block Chaining
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard
HMAC	Hash Message Authentication Code
MD5	Message Digest Algorithm 5
SSH	Secure Shell login using PuTTY.
CLI	Command Line Interface.

By:
Ashish Sharma
Senior SME