KillTest

高品質　より良いサービス

練習問題

https://www.killtest.jp

1年間無料アップデート

Exam : **NS0-594**

Title : NetApp Support Engineer, ONTAP Exam

Version : DEMO

1.A volume uses mixed security style. A directory in the volume previously had NTFS effective security after an SMB administrator applied an NTFS ACL. An NFSv3 administrator then changed the mode bits on that same directory. SMB users who had access through the NTFS ACL can no longer open files in the directory.
What explains the change in access?
A. The export policy superseded the SMB share and file ACLs.
B. The directory now uses UNIX effective security.
C. ONTAP converted the entire volume from mixed security style to UNIX security style.
D. The SMB server stopped applying file-level authorization checks to that directory.
Answer: B
Explanation:
On a mixed-security-style volume, the effective security style is determined at the file or directory level. When an NFSv3 client modifies permissions, the affected object uses UNIX mode bits and therefore has UNIX effective security. The volume itself remains mixed, so option C is incorrect. Export policy evaluation does not replace SMB share or file-level authorization, which eliminates option A. SMB clients can access data with UNIX effective security when authentication, name mapping, and UNIX permissions allow it; ONTAP does not stop performing file-level authorization as described in option D.
Reference: Learn about ONTAP NAS security styles

2.An NFS client mounted a volume successfully while its export policy rule used the client's IP address in `-clientmatch`. After the rule was changed to use the client's hostname, new mount attempts are denied. Restoring the IP address immediately restores access. A DNS query initiated from the data SVM cannot resolve the client hostname.
What should the support engineer do first?
A. Restore DNS service for the data SVM and verify resolution of the client hostname.
B. Replace the rule with a netgroup and configure an NIS domain on the data SVM.
C. Move the NFS data LIF to a port on the node that owns the volume's aggregate.
D. Add a local UNIX user with a UID matching the account presented by the NFS client.
Answer: A
Explanation:
ONTAP uses the DNS configuration of the data SVM when it must resolve certain hostname-based client matches. The IP-based rule works, the hostname-based rule fails, and name resolution from the SVM is unsuccessful, so DNS service for the SVM is the first issue to correct. A netgroup would change the matching design without resolving the demonstrated DNS failure. Data LIF placement relative to the aggregate owner does not determine whether a hostname matches an export rule. UNIX user lookup occurs after the client has matched the rule and does not explain why changing only `-clientmatch` caused the failure.
Reference: Add a rule to an ONTAP NFS export policy

3.An NFS user named `analytics` is denied access to a directory in a mixed-security-style volume. The client matches an export policy rule that permits read-write access, and the directory's UNIX mode bits permit the requested operation. Storage-Level Access Guard is also applied to the volume and grants access to `CORP\analytics`. A name-mapping check shows that the UNIX user `analytics` does not map to a Windows identity.

What should the support engineer correct?
A. Repair the UNIX-to-Windows mapping so `analytics` maps to the permitted CORP identity.
B. Change the volume from mixed to NTFS security style before allowing NFS access.
C. Remove Storage-Level Access Guard because it is evaluated only for SMB sessions.
D. Modify the export rule to grant superuser access to the address of the NFS client.
Answer: A
Explanation:
Storage-Level Access Guard is an additional authorization layer that applies to NAS access, including NFS. Because it uses NTFS permissions, a UNIX user must map to a Windows identity before ONTAP can evaluate the user against the Storage-Level Access Guard ACL. Repairing the mapping to the permitted CORP identity addresses the failed authorization. Converting the volume to NTFS security style is unnecessary. Storage-Level Access Guard is not limited to SMB, and export-policy superuser handling does not replace the required identity mapping or the Storage-Level Access Guard check.
Reference: Learn about secure ONTAP SMB file access by using Storage-Level Access Guard

4.The `system health status show` command reports a degraded state. A support engineer needs to identify the active alert, the affected resource, the probable cause, and the corrective actions recorded by ONTAP.
Which command provides the required details?
A. `system health config show -instance`
B. `system health alert definition show -instance`
C. `system health alert show -instance`
D. `system health subsystem show -instance`
Answer: C
Explanation:
`system health alert show -instance` displays detailed information about generated alerts, including the node, resource, severity, probable cause, possible effect, and corrective actions. `system health config show -instance` describes health-monitor configuration and status. `system health alert definition show -instance` displays alert definitions that the health monitors can generate, not the currently active alert instances. `system health subsystem show -instance` reports aggregated subsystem health and outstanding-alert counts but does not provide the full active-alert details requested.
Reference: Commands for monitoring the health of your ONTAP system

5.A node has rebooted after a panic. Technical support wants to determine whether the core dump is still being saved and, if so, review the number of blocks already written.
Which command should the support engineer run?
A. `system node coredump config show`
B. `system node coredump reports show`
C. `system node coredump show -instance`
D. `system node coredump status`
Answer: D
Explanation:
`system node coredump status` reports the status of core dumps. When ONTAP is saving a dump

to a core file, the output includes the core file name, the total number of blocks to save, and the number already saved. The configuration command shows core-dump settings, while the reports command manages application core reports. `system node coredump show` provides basic information about core dump files but is not the command that reports the active save progress described in the scenario. Reference: system node coredump status