Passcert

Higher Quality, better service!

Q&A

Http://www.passcert.com

We offer free update service for one year.

Exam : **D-AXAZL-A-00**

Title : Dell AX System for Azure Local Implementation Achievement

Version : DEMO

1.A Support Engineer is investigating why a node takes a very long time (>30 minutes) to enter Maintenance Mode during a CAU run, triggering timeouts.
The engineer checks the Cluster Events and sees repeated warnings about "CSV ownership change" and "Virtual Machine Live Migration" occurring very slowly.
What underlying networking configuration should the engineer verify to ensure rapid Live Migration during updates?
A. Check whether the Windows Search service is actively indexing VHDX files on the Cluster Shared Volume, potentially causing disk I/O contention during migration operations.
B. In Failover Cluster Manager, verify Live Migration network settings prioritize RDMA (SMB Direct) adapters over management network adapters.
C. Ensure the Cluster Shared Volume (CSV) is set to Redirected Access mode, which routes all I/O through a single coordinator node and is unsuitable for optimal Live Migration performance.
D. Verify IPv6 is disabled on all cluster network interfaces across nodes, based on the outdated belief that IPv4-only configurations improve Live Migration traffic efficiency.
Answer: B

2.A Site Reliability Engineer is verifying the switch configuration for a new Dell AX deployment. The engineer runs a command on the Top-of-Rack switch to verify the Quality of Service settings for the RDMA traffic class (Priority 3).
Refer to the following switch command output:
Switch# show dcb ets details

Interface	Priority-Group	Priority	Bandwidth (%)
Eth1/1	0	0,1,2,4-7	40%
Eth1/1	1	3	60%

Switch# show dcb pfc details

Interface	Priority	Status
Eth1/1	3	Disabled
Eth1/1	0-2,4-7	Disabled

Based on this output, what is the critical configuration error that will impact the stability of the Azure Local storage fabric?
A. Priority 3 is assigned to a dedicated Priority Group, preventing bandwidth borrowing from other traffic groups during congestion events.
B. The bandwidth allocation for Priority Group 1 is set to 60%, which exceeds the Microsoft recommended maximum of 50%.
C. Using Priority 0 for non-storage traffic conflicts with standard management traffic class assignments in converged fabric designs.
D. Priority Flow Control (PFC) is disabled for Priority 3 (the designated RDMA traffic class), violating the mandatory lossless network fabric requirement essential for reliable RoCEv2 operation in Azure Local storage environments.

Answer: D

3.A Network Administrator is working with a Deployment Engineer to resolve a complex connectivity failure during the "Register with Azure Arc" phase.
- Seed 1 (Firewall Rule): The firewall is configured to allow TCP 443 to *.azure.com and *.microsoftonline.com.
- Seed 2 (Agent Behavior): The azcmagent is failing with a timeout error when attempting to reach the Hybrid Identity Service.

```
# PowerShell Test-NetConnection Result (from Node-01)
PS C:\> Test-NetConnection -ComputerName gbl.his.arc.azure.com -Port 443
 WARNING: TCP connect to (20.120.10.5 : 443) failed
 ComputerName : gbl.his.arc.azure.com
 RemoteAddress : 20.120.10.5
 RemotePort : 443
 InterfaceAlias : vEthernet (Mgmt)
 SourceAddress : 10.20.10.5
 PingSucceeded : False
 TcpTestSucceeded : False
# Firewall Log Snippet
  Feb 20 10:15:22 FW-01 Deny TCP 10.20.10.5:49152 -> 20.120.10.5:443 (Rule: Default-Deny)
 Feb 20 10:15:23 FW-01 Allow TCP 10.20.10.5:49153 -> 13.107.6.156:443 (Rule: Allow-Azure-Mgmt)
```

Based on the interaction between the firewall rules and the agent's connection attempt, what is the root cause of the failure and the required remediation? (Select all that apply.)
A. Firewall rule Allow-Azure-Mgmt permits *.azure.com, yet the endpoint gbl.his.arc.azure.com resolves to an IP not recognized by the firewall's FQDN filter due to DNS mismatch or absence of real-time FQDN-to-IP mapping capability.
B. The remediation requires configuring firewall rules to explicitly allow the "AzureArc" and "AzureActiveDirectory" Service Tags, which dynamically include all required IP ranges and eliminate reliance on fragile FQDN-only filtering.
C. The firewall log shows a Deny for IP 20.120.10.5. Without Service Tag support, the firewall cannot associate this dynamic Azure IP with the permitted FQDN, causing a block at Layer 3/4 before Layer 7 inspection occurs.
D. The Test-NetConnection failure does not indicate a node-local routing issue; the Default-Deny log entry from FW-01 confirms traffic traversed the network and was blocked at the firewall, confirming a firewall policy problem.
E. The azcmagent uses ephemeral source port 49152, which is standard behavior for outbound connections. Firewalls evaluate destination port (443) for outbound rules; source port restrictions are neither required nor standard practice.
Answer: B, C

4.An Implementation Engineer is executing the azcmagent connect command to onboard a node to Azure Arc.
Which specific set of command-line parameters is mandatory for a successful registration using a Service Principal, assuming no local configuration files are pre-populated?

A. --client-id, --client-secret, --tenant-id, --url (Note: azcmagent requires --service-principal-id and --service-principal-secret; these generic OAuth parameters are invalid for Azure Arc registration)
B. --subscription-id, --tenant-id, --location, --resource-group (When credential parameters are omitted, this set initiates Interactive Login using the device code authentication flow)
C. --subscription-id, --tenant-id, --location, --resource-group, --access-token (Access tokens are short-lived, require external generation, and are not the standard method; Service Principal credentials are recommended for automation)
D. --subscription-id, --tenant-id, --location, --resource-group, --service-principal-id, --service-principal-secret
Answer: D

5.Why is attempting to rename the computer and join the domain in the same unattend.xml pass often considered a reliability Anti-Pattern? (Choose 2.)
A. The Windows Time Service (W32Time) cannot synchronize with the Domain Controller if the computer name has changed but the system has not rebooted, due to transient hostname resolution states during deployment workflows.
B. Azure Arc registration may fail when a pending computer name change exists in the registry, as the process requires a stable, reboot-applied hostname for successful onboarding.
C. If domain join succeeds but rename fails, the system joins the domain using a random name. Resolution requires unjoining, renaming, and rejoining to correctly update SPN records.
D. Domain join depends on the NetBIOS name, which may not update until after the rename reboot. This can cause the computer account to be created with the old random name (WIN-XXXX).
E. Secure Boot, a UEFI firmware security feature validating boot integrity, prevents simultaneous modification of the hostname and machine account password during Windows OOBE deployment phases.
Answer: C, D