Failover Clustering Interview Guide

This guide contains questions based on the provided articles covering Failover Clustering concepts, recovery mechanisms, configuration, and troubleshooting. Use the marking criteria to evaluate the candidate's understanding.

Easy Questions (Direct Recall / Basic Concepts)

#	Question	Marking Criteria (Scale of 1-10)
E1	What is the Resource Hosting Subsystem (RHS)?	Focuses on whether the candidate recalls its basic function. • 1-4: Incorrect / Vague (e.g., "part of clustering"). • 5-7: Mentions it hosts resources OR runs resource DLLs. • 8-10: Clearly states it's the process that hosts resource DLLs and interacts with them (e.g., calling entry points like IsAlive).
E2	What are the default time intervals for the LooksAlive and IsAlive health checks?	Tests recall of specific default values. • 1-4: Incorrect values or doesn't know. • 5-7: Correctly identifies one interval. • 8-10: Correctly identifies both (LooksAlive: 5 seconds, IsAlive: 60 seconds).
E3	What is the default value for the `DeadlockTimeout` common property?	Tests recall of a specific default timeout. • 1-4: Incorrect value or doesn't know. • 5-7: Knows it's measured in minutes but gets the value wrong. • 8-10: Correctly states 5 minutes (or 300000 milliseconds as shown in the PowerShell example).
E4	What event ID indicates that cluster health detection is attempting recovery by terminating the RHS process for an unresponsive resource?	Tests recall of a specific event ID. • 1-4: Incorrect ID or doesn't know. • 5-7: Mentions related event IDs like 1146 but not 1230. • 8-10: Correctly identifies Event ID 1230.
E5	What is the primary purpose of a Failover Cluster?	Tests understanding of the fundamental goal. • 1-4: Vague or incorrect (e.g., "makes servers faster"). • 5-7: Mentions high availability OR redundancy OR minimizing disruptions. • 8-10: Clearly states it's to increase the availability of applications and services by providing failover capabilities.

#	Question	Marking Criteria (Scale of 1-10)
E6	In Failover Clustering, what are 'nodes'?	Tests understanding of basic terminology. • 1-4: Incorrect definition. • 5-7: Describes them as computers in the cluster. • 8-10: Defines them as the independent servers/computers that are members of the cluster and work together.
E7	What file system format is recommended for cluster storage volumes, including the witness disk?	Tests recall of storage configuration recommendation. • 1-4: Incorrect format (e.g., FAT32, ReFS) or doesn't know. • 5-7: Mentions NTFS but isn't sure if it applies to witness disks. • 8-10: Correctly states NTFS is recommended for both data volumes and required for witness disks.
E8	What event ID typically indicates that one or more cluster nodes were removed from active failover cluster membership?	Tests recall of a key troubleshooting event ID. • 1-4: Incorrect ID or doesn't know. • 5-7: Mentions other cluster event IDs but not 1135. • 8-10: Correctly identifies Event ID 1135.
E9	What are the two primary settings mentioned that affect cluster heartbeating and health detection between nodes?	Tests recall of key heartbeat tuning parameters. • 1-4: Incorrect settings or doesn't know. • 5-7: Correctly identifies one (Delay or Threshold). • 8-10: Correctly identifies both Delay and Threshold.
E10	What tool is used to install the Failover Clustering feature on Windows Server?	Tests recall of the basic installation method shown. • 1-4: Incorrect tool or doesn't know. • 5-7: Mentions PowerShell but not the GUI tool shown. • 8-10: Correctly identifies Server Manager (Add Roles and Features).

Medium Questions (Synthesis / Implications)

#	Question	Marking Criteria (Scale of 1-10)
M1	Explain the difference in purpose between the LooksAlive and IsAlive health checks.	Tests understanding of the roles of the two checks. • 1-4: Confuses the two or description is inaccurate. • 5-7: Describes one correctly OR correctly states one is lightweight/frequent and the other is thorough/less frequent. • 8-10: Clearly explains LooksAlive is a quick, frequent check, while IsAlive is a more comprehensive check triggered less often or after a LooksAlive failure. States IsAlive failure determines resource failure.

#	Question	Marking Criteria (Scale of 1-10)
M2	What is the consequence if a resource fails its LooksAlive check but passes the subsequent IsAlive check?	Tests understanding of the health check sequence and outcome. • 1-4: Incorrectly states the resource fails or RHS restarts. • 5-7: States that IsAlive is called but unsure of the outcome. • 8-10: Correctly explains that RHS calls IsAlive after a LooksAlive failure, and if IsAlive passes, the resource is considered healthy and no recovery action is taken.
M3	Before Windows Server 2012, what was the impact on other healthy resources if the RHS process hosting them terminated due to one unresponsive resource?	Tests understanding of the impact of RHS termination in older versions. • 1-4: Incorrect impact described or doesn't know. • 5-7: Mentions other resources might be affected but unsure how. • 8-10: Clearly states that all resources hosted in that specific RHS process would also be terminated and restarted, causing an outage for them (using the 5 VM example from the text is a plus).
M4	How did the 'Resource Re-attach' feature in Windows Server 2012 improve RHS recovery?	Tests knowledge of specific improvements. • 1-4: Incorrect description or confuses it with resource isolation. • 5-7: Vaguely mentions it reduced impact or made recovery better. • 8-10: Explains that healthy resources in a recycled RHS process could re-attach to the new RHS process without restarting, minimizing the impact of a single resource failure.
M5	Briefly describe the 'Node and Disk Majority' quorum configuration mentioned in the context of a two-node cluster.	Tests understanding of a specific quorum type. • 1-4: Incorrect definition or confuses it with other quorum types. • 5-7: Mentions it uses nodes and a disk but explanation is weak. • 8-10: Explains that both the nodes and a dedicated witness disk hold copies of the cluster config, and the cluster remains online if a majority (more than half) of these voting elements are available.
M6	Explain the trade-off involved when deciding between Aggressive vs. Relaxed cluster network monitoring thresholds.	Tests understanding of the implications of tuning thresholds. • 1-4: Incorrectly describes the trade-off. • 5-7: Mentions one side of the trade-off (e.g., aggressive is faster for hard failures OR relaxed is better for transient issues). • 8-10: Clearly explains the balance: Aggressive provides faster recovery from hard failures but may cause unnecessary failovers during transient issues. Relaxed tolerates transient issues better but takes longer to recover from hard failures (increased downtime).
M7	How does setting the `SeparateMonitor` property for a resource help in managing cluster stability?	Tests understanding of this specific property's function. • 1-4: Incorrect explanation. • 5-7: Mentions it isolates the resource but unclear how or why. • 8-10: Explains that it forces the resource to run in its own dedicated RHS process, so if that resource hangs or crashes RHS, it won't affect other resources running on the node.

#	Question	Marking Criteria (Scale of 1-10)
M8	According to the articles, why is it highly recommended to validate a cluster configuration before creating the cluster?	Tests understanding of the purpose of validation. • 1-4: Vague reasons (e.g., "it's good practice"). • 5-7: Mentions checking configuration OR ensuring compatibility. • 8-10: Explains it confirms that the servers, network, and storage meet the specific requirements for failover clustering, ensuring compatibility and identifying potential issues *before* cluster creation, contributing to a stable and supported setup.
M9	Based on the troubleshooting scenarios for Event ID 1135, what does it likely indicate if all nodes in Site 1 log events for losing communication with all nodes in Site 2, and vice versa?	Tests ability to interpret a specific troubleshooting scenario. • 1-4: Incorrect interpretation (e.g., blames a single node). • 5-7: Suggests a network issue but is vague. • 8-10: Correctly identifies this pattern (Scenario B) as indicative of a communication failure over the link connecting the two sites (likely a WAN link issue).
M10	Why must network adapters used for iSCSI traffic be dedicated to that purpose and not shared with regular network communication in a failover cluster?	Tests understanding of network configuration best practices mentioned. • 1-4: Incorrect reason or doesn't know. • 5-7: Mentions performance OR reliability without specific context. • 8-10: Explains that dedicating adapters ensures predictable performance and avoids contention between storage I/O and regular network traffic, which is critical for storage stability and performance in a cluster.

Hard Questions (Application / Troubleshooting / Deeper Insight)

#	Question	Marking Criteria (Scale of 1-10)
H1	Describe the full sequence of events, including default timeouts, that occurs when a cluster resource (e.g., a Virtual Machine resource) becomes unresponsive during an IsAlive check, potentially leading up to a node bugcheck (STOP 0x9E).	Tests synthesis of the entire recovery process and timeouts. • 1-4: Sequence is incorrect or key steps/timeouts missing. • 5-7: Describes parts correctly (e.g., RHS waits DeadlockTimeout, terminates RHS) but misses the bugcheck step or timeout multiplication. • 8-10: Accurately details the sequence: 1. RHS calls IsAlive. 2. Resource doesn't respond. 3. RHS waits `DeadlockTimeout` (5 mins default). 4. If no response, Cluster Service requests RHS termination. 5. Cluster Service waits 4 * `DeadlockTimeout` (20 mins default) for RHS to terminate. 6. If RHS doesn't terminate, Cluster Service calls NetFT to bugcheck the node (STOP 0x9E, Parameter3 = 0x5).

#	Question	Marking Criteria (Scale of 1-10)
H2	Imagine a 5-node cluster where nodes frequently lose network connectivity for 15 seconds due to transient network congestion. The default `SameSubnetThreshold` is 10 (Win2016+ default). Would this cause nodes to be removed from the cluster? Explain how you might adjust thresholds (`SameSubnetDelay`, `SameSubnetThreshold`) to tolerate this, and state the primary risk of making this adjustment.	Tests application of threshold tuning to a scenario. • 1-4: Incorrect calculation or adjustment logic. Doesn't identify the risk. • 5-7: Correctly calculates the default tolerance (10 * 1s = 10s). Identifies this is *less* than 15s, meaning nodes *would* be removed. Suggests increasing the Threshold OR Delay but explanation of risk is weak. • 8-10: 1. Correctly calculates default tolerance (10 heartbeats * 1 second delay = 10 seconds). 2. States nodes *would* be removed as 15s > 10s. 3. Suggests increasing `SameSubnetThreshold` (e.g., to 20, giving 20s tolerance) OR increasing `SameSubnetDelay` (less preferred, e.g., to 2s giving 20s tolerance). Explains *why* increasing Threshold is generally preferred over Delay. 4. Clearly states the risk: increased time to detect and recover from *actual* hard failures, leading to longer downtime in those scenarios.
H3	You are investigating an issue where Event ID 1230 and 1146 occurred for a specific clustered resource. What steps would you take using the cluster log (`Get-ClusterLog`) to pinpoint the failure, considering time zone differences? What information are you looking for in the log?	Tests knowledge of practical troubleshooting steps using logs. • 1-4: Unsure how to use cluster log or what to look for. • 5-7: Mentions generating the log and looking for errors around the event time, but misses time zone handling or specific log entries. • 8-10: Describes the process: 1. Note the *local* time of Event ID 1230/1146. 2. Generate the cluster log using `Get-ClusterLog`. Use `-UseLocalTime` (on Win2012+) to simplify correlation, otherwise, convert event time to GMT. 3. Search the log around the failure time for entries related to the specific resource mentioned in Event 1230. 4. Look for log entries like `[RHS] RhsCall::DeadlockMonitor: Call timed out for resource "` and `[RHS] Resource handling deadlock`. Identifies which entry point (e.g., ISALIVE) timed out.
H4	A customer wants to deploy a two-node file server cluster but only has one shared LUN available. Based on the prerequisites and quorum discussion, can they create a supported cluster? Explain why or why not, and suggest an alternative if applicable.	Tests understanding of storage prerequisites and quorum implications. • 1-4: Incorrectly states it's possible or explanation is wrong. • 5-7: Correctly states it's likely not supported but struggles to explain why (misses quorum requirement) OR suggests an invalid alternative. • 8-10: Explains that a two-node cluster typically requires at least two LUNs: one for the witness disk (for Node and Disk Majority quorum) and one for the data/file share. With only one LUN, they cannot configure the recommended quorum type for a two-node cluster. Suggests alternatives like using a File Share Witness (if another server is available) which doesn't require a dedicated LUN, or potentially using Node Majority quorum (less resilient for 2 nodes) if no witness is possible. (Cloud Witness is outside scope of articles but acceptable if mentioned).
H5	Explain why antivirus exclusions are critical for failover cluster stability, mentioning at least two specific paths or processes that should be excluded according to the article.	Tests understanding of the impact of AV and recall of specific exclusions. • 1-4: Vague answer about performance or doesn't recall specific exclusions. • 5-7: Explains AV can interfere with cluster operations (locking files, scanning memory) OR recalls one specific exclusion. • 8-10: Clearly explains that real-time scanning can interfere with cluster service operations, quorum disk access, or VM files, causing performance issues or unexpected failovers. Correctly names at least two exclusions mentioned: `%Systemroot%\Cluster` folder, the File Share Witness path (if used), `C:\ClusterStorage`, `mms.exe`, or `vmwp.exe`.

#	Question	Marking Criteria (Scale of 1-10)
H6	If you configure a resource to run with `SeparateMonitor = 1`, what is the primary resource cost associated with this change, according to the article?	Tests understanding of the implication of using SeparateMonitor. • 1-4: Incorrect cost mentioned (e.g., performance hit, disk space). • 5-7: Mentions increased resource usage but is vague. • 8-10: Correctly states that each dedicated RHS process consumes additional system resources, specifically mentioning a small amount of RAM (a few MB per process) as observed in Task Manager.
H7	The troubleshooting guide mentions checking the 'Network Interface\Packets Received Discarded' performance counter. What might cause this counter to be higher than zero, and why is this relevant to cluster heartbeat failures (Event ID 1135)?	Tests understanding of a specific performance counter and its relevance. • 1-4: Incorrect cause or relevance. • 5-7: Mentions packet loss but unsure of the cause OR correctly identifies a cause (e.g., insufficient receive buffers) but unclear on relevance to heartbeats. • 8-10: Explains that a non-zero value indicates the network adapter is discarding incoming packets, often due to insufficient receive buffers on the NIC, especially during traffic bursts. This is relevant because if heartbeat packets are among those discarded, nodes will fail to communicate, leading to perceived failures and Event ID 1135 (node removal).
H8	What permissions does the account used to initially create a cluster need in Active Directory if it's not a Domain Admin account?	Tests understanding of AD prerequisites for cluster creation. • 1-4: Incorrect permissions or states Domain Admin is required. • 5-7: Mentions needing computer object permissions but is vague. • 8-10: Correctly states the account (or a group it's in) needs 'Create Computer Objects' and 'Read All Properties' permissions in the Organizational Unit (OU) where the cluster nodes reside (or where the Cluster Name Object will be created). Also acceptable: Administrator rights on the cluster node servers themselves.
H9	How does the cluster handle a disk designated as part of a clustered file server role differently than a non-clustered disk when you try to create a share on it using standard Windows tools like Explorer?	Tests understanding of how cluster integration affects standard operations. • 1-4: States there is no difference or description is incorrect. • 5-7: Mentions the cluster recognizes the disk but explanation is weak. • 8-10: Explains that Windows (Explorer, Share and Storage Mgmt snap-in) recognizes the disk is part of cluster storage. If the disk is already configured within a clustered file server role, sharing works normally via these tools. If the disk is *not* yet configured in the role, attempting to share it directly will result in an error, prompting the user to configure it within the Failover Cluster Manager first.
H10	A cluster node fails to rejoin the cluster after a reboot. Event ID 1135 is logged by other nodes indicating the failed node was removed. Besides network issues, what specific Windows service on the failed node should be checked first as a potential cause, according to the Event ID 1135 text?	Tests ability to extract key troubleshooting info from event text. • 1-4: Names incorrect service or focuses only on network. • 5-7: Mentions checking services generally. • 8-10: Correctly identifies the 'Cluster Service' (ClusSvc) as the primary service to check on the failed node, as its stoppage is explicitly mentioned in the Event ID 1135 description as a possible cause.