

Refer To The Exhibit. Serverb Is Attempting To Contact Hosta. Which Two Statements Correctly Identify

Refer To The Exhibit. Serverb Is Attempting To Contact Hosta. Which Two Statements Correctly Identify the key details of this networking scenario? When analyzing server communication issues or network configurations, understanding the specifics of how servers interact, what protocols are involved, and the underlying network topology is crucial. This article aims to clarify the two correct statements regarding Serverb's attempt to contact Hosta, providing insights into network troubleshooting, server roles, and communication protocols relevant to this scenario.

Understanding the Context of Server-Host Communication

What Is the Significance of the Exhibit?

The exhibit provides a visual or diagrammatic representation of the network setup, including servers, hosts, routers, and other network devices. It typically displays IP addresses, port numbers, protocols, and the path taken by data packets. Analyzing this exhibit helps identify potential issues such as connectivity failures, misconfigurations, or security restrictions affecting Serverb's attempt to reach Hosta.

Common Scenarios in Server-Host Communications

Servers often communicate with hosts using various protocols such as TCP/IP, HTTP, DNS, or others depending on their roles. Failures in such communications may stem from:

- Incorrect network configurations
- Firewall or security rules blocking traffic
- DNS resolution issues
- Network congestion or hardware failures

Understanding these aspects is vital to accurately interpret the exhibit and determine which statements correctly describe the situation.

Key Statements About Serverb Contacting Hosta

In analyzing the exhibit, two statements typically emerge as correct explanations of the scenario. These are:

Statement 1: Serverb Is Using the Correct Protocol to Initiate Communication

This statement indicates that Serverb attempts to contact Hosta utilizing the appropriate protocol, such as TCP for reliable transmission or UDP for faster, connectionless communication. Confirming the protocol is essential because:

- It ensures that Serverb's request aligns with Hosta's listening services.
- It explains whether the connection attempt should succeed under normal circumstances.
- It helps determine if protocol mismatches or port issues are causing failures.

For example, if Serverb is trying to establish an HTTP connection on port 80 or 443, and the exhibit shows that Hosta is listening on that port, then the protocol use is appropriate. Conversely, if Serverb is attempting to connect via SSH (port 22) but Hosta does not have SSH enabled, the attempt would fail despite the correct protocol.

Statement 2: There Is a Network Connectivity Issue Between Serverb and Hosta

The second valid statement often relates to network connectivity problems. These can include:

- Routing issues preventing packets from reaching Hosta
- Firewall rules blocking traffic on specific ports
- Physical connectivity problems such as faulty cables or network hardware
- Incorrect IP address configurations leading to packets being sent to the wrong destination

The exhibit may highlight issues like:

- No response packets received from Hosta
- Ping failures indicating unreachable hosts
- Traceroute results showing a break in the network path

Identifying a connectivity issue explains why Serverb cannot establish communication, even if the protocol and port configurations are correct.

Additional Important Considerations in the Scenario

Role of DNS Resolution

Sometimes, the problem lies not in the network path but in resolving the hostname Hosta to its IP address. If Serverb is attempting to contact Hosta via its hostname, DNS resolution must succeed for the communication to proceed. The exhibit may show:

- Successful DNS resolution with the correct IP address
- Failure in DNS resolution leading to an inability to locate Hosta

Understanding whether DNS issues are involved helps clarify if the problem is at the application layer or the network layer.

Firewall and Security Settings

Firewalls on Serverb, Hosta, or intermediate devices can block traffic based on rules. The exhibit might indicate:

- Open ports allowing communication
- Blocked ports preventing contact
- Security policies that restrict server-to-host communication

Correctly identifying security restrictions is crucial for determining why Serverb cannot reach Hosta, even if network connectivity and protocol configurations are correct.

Summary of the Two Correct Statements

Based on the analysis of typical network scenarios reflected in the exhibit, the two correct statements are:

- **Serverb Is Using the Correct Protocol To Contact Hosta:** This confirms that the protocol and port used by Serverb align with Hosta's listening services, indicating that protocol mismatch is not the cause of the communication failure.
- **There Is a Network Connectivity Issue Between Serverb and Hosta:** This suggests that physical, routing, or firewall issues are preventing packets from reaching Hosta, explaining the failed or incomplete communication attempt.

These statements collectively help network administrators diagnose and resolve the issue effectively, ensuring that Serverb can successfully contact Hosta in future attempts.

Conclusion

Understanding the scenario where Serverb attempts to contact Hosta is essential in network management and troubleshooting. The exhibit offers vital clues, and recognizing the correct statements—namely, that

Serverb uses the appropriate protocol and that there is a network connectivity problem—guides effective problem-solving. Remember, network issues can stem from a variety of factors, but focusing on protocol correctness and connectivity status provides a solid foundation for resolving communication failures. Whether you are a network administrator, cybersecurity professional, or IT student, mastering these concepts is key to maintaining robust and efficient network operations.

Frequently Asked Questions

What does the exhibit indicate about Serverb's attempt to contact Hosta?

The exhibit shows that Serverb is trying to establish a connection with Hosta, likely to access resources or services hosted on Hosta.

Which two statements correctly identify the possible reasons for Serverb's contact attempt with Hosta?

One reason could be that Serverb is requesting data or services hosted on Hosta, and another could be that Serverb is performing health checks or status updates.

Based on the exhibit, what network protocols might Serverb be using to contact Hosta?

Serverb could be using protocols such as TCP/IP, HTTP/HTTPS, or other application-layer protocols depending on the nature of the communication depicted.

What implications does Serverb's attempt to contact Hosta have for network security?

It could indicate normal operation, but if unexpected, it may also suggest a potential security concern like unauthorized access or a compromised server attempting to communicate.

Which two statements correctly interpret the significance of the contact attempt shown in the exhibit?

First, it signifies an active network connection attempt between Serverb and Hosta. Second, it may reflect scheduled maintenance, application requests, or troubleshooting activities.

Additional Resources

Refer To The Exhibit. Serverb Is Attempting To Contact Hosta. Which Two Statements Correctly Identify

When analyzing network connectivity issues, particularly in a complex environment involving servers and hosts, understanding the underlying communication protocols and configurations is essential. The phrase "Refer To The Exhibit" suggests that a specific network diagram or output is provided, illustrating the interaction between Serverb and Hosta. The scenario indicates that Serverb is attempting to establish contact with Hosta, and the goal is to determine which statements accurately describe this process. This kind of problem is typical in troubleshooting network environments, especially when diagnosing communication failures, verifying configurations, or understanding traffic flow. This article will explore the key aspects involved in such scenarios, including the network protocols, possible reasons for contact attempts, and the correct interpretations of the situation, supported by detailed analysis and explanations.

Understanding the Context of Serverb Attempting to Contact Hosta

Before diving into the specific statements, it's important to grasp the context of the problem. When a server such as Serverb attempts to contact a host like Hosta, it could be for various reasons: establishing a connection, verifying availability, transmitting data, or performing a network service request. The process involves several layers of the OSI model, primarily focusing on the network and transport layers.

In typical enterprise networks, such attempts could be initiated via protocols like TCP/IP, UDP, or application-layer protocols such as HTTP, FTP, or SSH. The nature of the attempt—whether it's a ping, a TCP connection, or a specific application request—affects how the communication is perceived and interpreted.

The "Refer To The Exhibit" phrase indicates that specific data, such as packet captures, configuration settings, or network diagrams, are provided. These details help identify whether the attempt is successful, blocked, or misconfigured. For instance, if the exhibit shows a TCP SYN packet from Serverb to Hosta, this suggests an attempt to initiate a connection at the TCP layer.

Analyzing the Two Correct Statements

In troubleshooting scenarios like this, two statements are often provided to explain or clarify the nature of

the contact attempt. The correctness of these statements depends on the network configuration, protocols involved, and observed behavior.

Let's explore typical statements that might be presented and analyze their correctness:

Statement 1: "Serverb is performing a DNS query to resolve Hosta's IP address."

Analysis:

This statement suggests that Serverb's attempt to contact Hosta begins with a Domain Name System (DNS) resolution process. This is common in network communication because servers often initiate contact using hostnames rather than IP addresses. The process involves the following steps:

- Serverb sends a DNS query to a DNS server, requesting the IP address associated with Hosta's hostname.
- If the DNS response is successful, Serverb proceeds to contact Hosta directly via the resolved IP address.

Supporting Evidence:

- If the exhibit shows DNS traffic from Serverb to a DNS server, with a subsequent response containing Hosta's IP, this confirms the DNS resolution process.
- If the initial packet from Serverb is a DNS query, and no TCP or UDP traffic is observed yet, this indicates that the contact attempt is at the DNS level.

Pros:

- Clarifies the initial step in establishing contact, especially if hostnames are used.
- Explains why DNS traffic appears before actual contact attempts.

Cons:

- Not all contact attempts involve DNS resolution; sometimes, IP addresses are hardcoded.
- If the exhibit shows that Serverb already knows Hosta's IP, this statement may not be applicable.

Conclusion:

This statement is correct if the exhibit indicates a DNS query initiated by Serverb. It accurately describes the initial phase of contact, especially in environments where hostnames are used.

Statement 2: "Serverb's attempt to contact Hosta is blocked by a firewall, preventing the TCP handshake."

Analysis:

This statement implies that although Serverb is attempting to establish a connection with Hosta, a firewall is actively blocking this traffic, resulting in failed connection attempts. The typical evidence includes:

- TCP SYN packets sent from Serverb to Hosta that do not receive SYN-ACK responses.
- Possible logs showing dropped packets or firewall rules denying traffic.

Supporting Evidence:

- The exhibit might display TCP connection attempts with no response, indicating blockage.
- Firewall logs or configurations in the exhibit could confirm rules that block specific ports or IP addresses.

Pros:

- Explains potential reasons for failed connection attempts.
- Highlights the importance of security controls in network environments.

Cons:

- If the exhibit shows successful TCP handshakes or no indication of blockage, this statement would be incorrect.
- Not all failed attempts are due to firewalls; other issues like network misconfigurations or host issues could be involved.

Conclusion:

This statement is correct if the exhibit's data indicates that connection attempts are unsuccessful due to firewall rules. It reflects a common scenario where security policies inadvertently block legitimate traffic.

Additional Factors to Consider in the Analysis

When analyzing such network scenarios, several other factors can influence whether the statements are correct:

- Network Topology: Understanding whether Serverb and Hosta are on the same subnet or different networks affects how contact attempts proceed.
- Routing Configurations: Proper routing ensures that packets reach the destination; misconfigurations can cause attempts to fail.
- Service Availability: Hosta must be configured to accept connections on the relevant port and protocol.
- Security Policies: Firewall rules, access control lists (ACLs), and intrusion detection systems can influence contact attempts.

Features and Pros/Cons of Correct Statements

Feature	Pros	Cons
---------	------	------

---	---	---
-----	-----	-----

DNS Query Explanation	Clarifies initial contact process; useful in hostname-based communication	Not applicable if IPs are static and directly used
-----------------------	---	--

Firewall Blockage Explanation	Explains common cause of failed connection; highlights security controls	May not apply if no evidence of blockage
-------------------------------	--	--

Conclusion: Which Two Statements Are Correct?

Based on typical network troubleshooting principles and assuming the exhibit shows relevant data, the two correct statements are:

1. Serverb is performing a DNS query to resolve Hosta's IP address — if the exhibit reveals DNS traffic preceding connection attempts or hostname resolution activity, this statement is valid. It correctly describes the initial phase of establishing communication, especially in environments where hostnames are used.
2. Serverb's attempt to contact Hosta is blocked by a firewall, preventing the TCP handshake — if network captures or logs evidence TCP SYN packets without responses, or if firewall rules are configured to block such attempts, this statement accurately explains why the contact is unsuccessful.

In sum, these two statements collectively cover the initial DNS resolution process and potential security barriers, providing a comprehensive understanding of the contact attempt scenario.

Final Thoughts

Troubleshooting network contact issues requires a detailed understanding of protocols, network configurations, and security policies. Analyzing exhibit data—such as packet captures, configuration diagrams, or logs—is crucial in confirming the accuracy of statements. Recognizing whether DNS resolution occurs or if firewalls are blocking traffic helps network administrators diagnose and resolve communication problems efficiently. Always consider the broader context, including network topology and security policies, when interpreting such scenarios to ensure accurate diagnoses and effective solutions.

Refer To The Exhibit Serverb Is Attempting To Contact Hosta Which Two Statements Correctly Identify

Refer To The Exhibit Serverb Is Attempting To Contact Hosta Which Two Statements Correctly Identify

Related Articles

- [Over The Past 500 Years, The Average Number Of Deaths Globally Due To Earthquakes Has Been _____ Per](#)
- [Read The Excerpt From Act 2, Scene 1, Of The Tragedyof Julius Caesar.BRUTUS. It Must Be By His Death:](#)
- [Please Help ASAP!Lisa Is Thinking About A Career In Hospitality And Tourism. She Has Always Wanted To](#)

[Back to Home](#)