SAS Institute
A00-250
A00-250 SAS Platform Administration for SAS9

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Which of the following operating system controls can be used to secure the SAS configuration directory by restricting access to specific users or groups?

A. File EMmissions
B. Access Control Lists (ACLs)
C. User accounts and group memberships
D. Firewall rules
E. Data encryption

Answer: A,B,C

Explanation:
File permissions, Access Control Lists (ACLs), and User accounts and group memberships are operating system controls that can be used to restrict access to the SAS configuration directory. File permissions allow you to specify which users or groups can read, write, or execute files and directories. ACLs provide a more granular level of access control. User accounts and group memberships allow you to assign specific permissions to users or groups. Firewall rules are used to control network traffic and are not directly related to securing the SAS configuration directory. Data encryption is a method of protecting data from unauthorized access, but it does not directly restrict access to the SAS configuration directory.

Question: 2

Which of the following statements about the SAS configuration directory is TRUE?

A. The SAS configuration directory is typically located in the letc/SAS directory.
B. The SAS configuration directory contains files that define the configuration of SAS software, such as the SAS system options and the SAS logon procedures.
C. The SAS configuration directory is only accessible to the SAS user account.
D. The SAS configuration directory is always encrypted by default.
E. The SAS configuration directory is a temporary directory that is deleted when SAS is shut down.

Answer: B

Explanation:
The SAS configuration directory contains files that define the configuration of SAS software, such as the SAS system options and the SAS logon procedures- The location of the SAS configuration directory varies depending on the operating system and the SAS installation- The SAS configuration directory can be accessed by users other than the SAS user account if the appropriate permissions are granted- The SAS configuration directory is not always encrypted by default, and encryption is a security measure that

should be considered. The SAS configuration directory is not a temporary directory and is persistent across SAS sessions.

Question: 3

You are a SAS administrator responsible for securing the SAS configuration directory on a Linux server. You want to ensure that only authorized users can access the directory. Which of the following commands can be used to set the permissions for the SAS configuration directory to allow only the 'sas' user to read and write?

A.
```
chmod 644 /etc/SAS
```

B.
```
chown sas:sas /etc/SAS
```

C.
```
chmod 700 /etc/SAS
```

D.
```
chown root:root /etc/SAS
```

E.
```
chmod 660 /etc/SAS
```

Answer: C

Explanation:
The command schmod 700 /etc/SAS' sets the permissions for the SAS configuration directory to allow only the 'sas user to read, write, and execute. The octal number 700 represents the following permissions: 'rwx—' (read, write, execute for the owner, and no permissions for others). Option A allows the owner to read and write, and others to read. Option B sets the owner and group to 'sas', but does not change the permissions. Option D sets the owner and group to 'root', which is not the desired outcome. Option E allows the owner and group to read and write, and others to write, which is not secure.

Question: 4

You are configuring the SAS configuration directory on a Windows server. Which of the following steps should you take to secure the directory by using operating system controls?

A. Set the directory permissions to 'Full Control' for the 'AdministratorS group.
B. Disable inheritance for the directory and remove all permissions except 'Read' for the 'Everyone' group.
C. Create a separate user account for SAS and grant it 'Full Control' permissions to the directory
D. Set the directory permissions to 'Read Only' for the 'System' user.

E. Enable the 'Encrypt contents to secure data' option for the directory.

Answer: C,E

Explanation:
The best way to secure the SAS configuration directory on a Windows server is to create a separate user account for SAS and grant it 'Full Control' permissions to the directory. This will limit access to the directory to only the SAS user account. Additionally, enabling the 'Encrypt contents to secure data' option for the directory will encrypt the files within the directory providing an additional layer of protection. Option A is too broad and could potentially allow unauthorized access to the directory. Option B will deny access to all users except the 'Everyone' group, which is not secure. Option D will deny access to the 'System' user, which could cause issues with SAS processes.

Question: 5

A SAS administrator wants to restrict access to the SAS configuration directory on a Unix server using file permissions. The administrator wants to allow only the SAS user (uid 1000) and the administrators group (gid 1 00) to have read and write access to the directory. Which of the following command lines would correctly set the permissions for the SAS configuration directory?

A.
```
chmod 660 /etc/SAS
```
B.
```
chmod 0660 /etc/SAS
```
C.
```
chmod 644 /etc/SAS
```
D.
```
chmod 770 /etc/SAS
```

E.
```
chmod 740 /etc/SAS
```

Answer: E

Explanation:
The correct command is 'chmod 740 /etc/SAS'. This command sets the permissions to 'rwxr—-' , giving the owner (SAS user) read, write, and execute permissions, the group (administrators) read permissions, and no permissions to others. Option A allows read and write for the owner and group, but not for others- Option B is invalid because the first digit must be between 0 and T Option C allows read only for the owner, group, and others. Option D allows read, write, and execute for the owner and group, and no permissions to others.

Question: 6

You are working as a SAS administrator. A new SAS user named 'newuser' needs to be able to access the SAS configuration directory. The SAS configuration directory is located in /etc/SAS. Which of the following commands will give 'newuser' read and execute permissions to the directory?

A.
```
chown newuser:newuser /etc/SAS
```
B.
```
chmod 755 /etc/SAS
```
C.
```
chmod +x /etc/SAS
```
D.
```
chmod +r /etc/SAS
```
E.
```
chmod 644 /etc/SAS
```

Answer: B

Explanation:
The correct command is 'chmod 755 letc/SAS. This command sets the permissions to 'rwxr-xr-x' , which grants the owner (SAS user) read, write, and execute permissions, the group (administrators) read and execute permissions, and others read and execute permissions. Option A sets the owner and group to 'newuser' but does not change the permissions. Option C adds execute permissions to the directory, but does not give read permissions. Option D adds read permissions to the directory but does not give execute permissions. Option E allows read only for the owner, group, and others.

Question: 7

You are a SAS administrator tasked with applying a critical hot fix to your SAS 9.4 environment. Which of the following actions should you perform BEFORE applying the hot fix?

A. Back up the SAS configuration files.
B. Restart the SAS server.
C. Run the SAS hot fix installation script.
D. Verify the hot fix is compatible with your SAS version.
E. Test the hot fix in a development environment.

Answer: A,D,E

Explanation:
Before applying a hot fix, it's crucial to back up your SAS configuration files to ensure a safe rollback option if needed. Verifying compatibility is essential to prevent potential conflicts or instability. Testing in a development environment allows you to assess the hot fix's impact before applying it to production.

Question: 8

You need to apply a hot fix to a specific SAS component, such as SAS/STAT. How can you apply the hot fix only to that component, minimizing potential disruptions to other SAS components?

A. Use the SAS Hot Fix Manager and select the specific component during installation.
B. Manually copy the hot fix files into the specific component's directory.
C. Apply the hot fix to the entire SAS installation and restart the server.
D. Use the SAS System Options to specify the hot fix for the particular component.
E. It's not possible to apply hot fixes to specific components in SAS 9.4.

Answer: A

Explanation:
The SAS Hot Fix Manager provides a mechanism to target specific SAS components for hot fix installations- This allows for selective updates, minimizing the risk of affecting unrelated components or causing unexpected behavior Options B, C, and D are incorrect as they involve less targeted approaches or are not valid methods.

Question: 9

Your SAS 9.4 system frequently experiences performance issues after applying hot fixes. What steps should you take to troubleshoot and prevent this recurring problem?

A. Monitor system logs for error messages related to the hot fixes.
B. Disable the SAS system options that are affected by the hot fix.
C. Contact SAS support for assistance in identifying the root cause.
D. Run performance tests before and after applying hot fixes to identify changes.
E. Reinstall SAS after each hot fix to ensure a clean installation.

Answer: A,C,D

Explanation:
Analyzing system logs for error messages related to the hot fixes can reveal the source of performance issues. Contacting SAS support provides expert guidance and potential solutions. Running performance tests before and after applying hot fixes helps identify changes in system behavior. Disabling system options might not address the root cause, and reinstalling SAS after every hot fix is inefficient and unnecessary.

Question: 10

You discover a recently applied hot fix has introduced a critical bug in your SAS 9.4 environment. Which of the following steps should you take immediately to mitigate the issue?

A. Contact SAS support to report the bug and request assistance.
B. Rollback the hot fix by restoring the previous configuration files.
C. Update the SAS system options to disable the functionality affected by the bug
D. Reinstall SAS 9.4 from scratch to eliminate the bug.
E. Wait for SAS to release a new hot fix addressing the bug

Answer: A,B

Explanation:
In a critical situation, contacting SAS support is essential to report the bug, get expert guidance, and potentially obtain a workaround or a faster solution. Rolling back the hot fix by restoring the previous configuration files is the quickest way to restore a stable environment. Options C, D, and E are less effective or involve more time-consuming actions, delaying the resolution of the critical bug.

Question: 11

Your SAS 9.4 environment has a large number of users and applications. You need to apply a hot fix that requires a server restart. What strategies can you implement to minimize downtime during the update process?

A. Apply the hot fix during off-peak hours when user activity is minimal.
B. Use a load balancer to distribute traffic across multiple servers, allowing updates on one server at a time.
C. Schedule the update during a planned maintenance window
D. Use the SAS Hot Fix Manager to apply the update in stages, restarting specific components.
E. Implement a rolling restart strategy where parts of the SAS server are restarted sequentially

Answer: A,B,C,E

Explanation:
Applying the hot fix during off-peak hours, utilizing a load balancer for traffic distribution, scheduling updates during maintenance windows, and implementing a rolling restart strategy are all effective ways to minimize downtime. The SAS Hot Fix Manager doesn't offer stage-by-stage updates with component-specific restarts.

Question: 12

You're reviewing the SAS 9.4 documentation for applying a critical hot fix related to a specific SAS/IML issue. You notice a warning that the hot fix may introduce a performance regression in certain scenarios. How should you approach this situation?

A. Ignore the warning and proceed with applying the hot fix, as the critical bug takes priority
B. Contact SAS support to confirm if the warning is accurate and request alternatives.
C. Apply the hot fix in a testing environment and conduct performance benchmarks to assess the impact
D. Delay the hot fix application until a new version of the SAS software is released.
E. Contact all users of SAS/IML to inform them about the potential performance regression.

Explanation:

Ifs crucial to contact SAS support for clarification regarding the performance regression warning. They can provide additional information, potential workarounds, or confirm if the warning is accurate. Testing the hot fix in a dedicated environment and conducting performance benchmarks is necessary to assess the actual impact and identify potential mitigation strategies. Ignoring the warning or delaying the fix might not be the best approach, while informing users about potential regressions is helpful but doesnt address the underlying issue.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/