

[2017 New Exam Collection SY0-401 Dumps And SY0-401 New Questions (251-275)]

2017 August CompTIA Official New Released SY0-401 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!

2017 get prepared with fully updated CompTIA SY0-401 real exam questions and accurate answers for SY0-401 exam. Lead2pass IT experts review the SY0-401 newly added questions and offer correct CompTIA SY0-401 exam questions answers. 100% pass easily! Following questions and answers are all new published by CompTIA Official Exam Center:

<https://www.lead2pass.com/sy0-401.html> QUESTION 251 Which of the following concepts defines the requirement for data availability? A. Authentication to RADIUS. B. Non-repudiation of email messages. C. Disaster recovery planning. D. Encryption of email messages. Answer: C. Explanation: A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses. QUESTION 252 Which of the following is the MOST specific plan for various problems that can arise within a system? A. Business Continuity Plan. B. Continuity of Operation Plan. C. Disaster Recovery Plan. D. IT Contingency Plan. Answer: D. Explanation: An IT contingency plan would focus on the IT aspect in particular to ensure business continuity. QUESTION 253 Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration? A. A disk-based image of every computer as they are being replaced. B. A plan that skips every other replaced computer to limit the area of affected users. C. An offsite contingency server farm that can act as a warm site should any issues appear. D. A back-out strategy planned out anticipating any unforeseen problems that may arise. Answer: D. Explanation: A backout is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout. QUESTION 254 Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency? A. Business continuity planning. B. Continuity of operations. C. Business impact analysis. D. Succession planning. Answer: D. Explanation: Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions. QUESTION 255 Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete? A. Succession planning. B. Disaster recovery. C. Separation of duty. D. Removing single loss expectancy. Answer: A. Explanation: Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions. QUESTION 256 Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following? A. Fault tolerance. B. Succession planning. C. Business continuity testing. D. Recovery point objectives. Answer: B. Explanation: Succession planning outlines those internal to the organization that has the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions. QUESTION 257 A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts? A. High availability. B. Load balancing. C. Backout contingency plan. D. Clustering. Answer: A. Explanation: High availability (HA) refers to the measures used to keep services and systems operational during an outage. In short, the goal is to provide all services to all users, where they need them and when they need them. With high availability, the goal is to have key services available 99.999 percent of the time (also known as five nines availability). QUESTION 258 A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate? A. Authentication. B. Integrity. C. Confidentiality. D. Availability. Answer: D. Explanation: Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected.

This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability.

QUESTION 259 The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand? A. Warm site implementation for the datacenter B. Geographically disparate site redundant datacenter C. Localized clustering of the datacenter D. Cold site implementation for the datacenter Answer: B Explanation: Data backups, redundant systems, and disaster recovery plans all support availability. AN in this case a geographically disparate site redundant datacenter represents 100% availability regardless of whether a disaster event occurs.

QUESTION 260 A company replaces a number of devices with a mobile appliance, combining several functions. Which of the following descriptions fits this new implementation? (Select TWO). A. Cloud computing B. Virtualization C. All-in-one device D. Load balancing E. Single point of failure Answer: CE Explanation: The disadvantages of combining everything into one include a potential single point of failure, and the dependence on the one vendor. The all ?n-one device represents a single point of failure risk being taken on.

QUESTION 261 A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost? A. Clustering B. Mirrored server C. RAID D. Tape backup Answer: CE Explanation: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

QUESTION 262 Which of the following may significantly reduce data loss if multiple drives fail at the same time? A. Virtualization B. RAID C. Load balancing D. Server clustering Answer: B Explanation: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

QUESTION 263 Which of the following provides data the best fault tolerance at the LOWEST cost? A. Load balancing B. Clustering C. Server virtualization D. RAID 6 Answer: DE Explanation: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software thus representing the lowest cost option.

QUESTION 264 Which of the following provides the LEAST availability? A. RAID 0 B. RAID 1 C. RAID 3 D. RAID 5 Answer: A Explanation: RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID 0 is disk striping. It uses multiple drives and maps them together as a single physical drive. This is done primarily for performance, not for fault tolerance. If any drive in a RAID 0 array fails, the entire logical drive becomes unusable.

QUESTION 265 Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent? A. Warm site B. Load balancing C. Clustering D. RAID Answer: CE Explanation: Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy. Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

QUESTION 266 After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage? A. Whole disk encryption B. Removable disk encryption C. Database record level encryption D. File level encryption Answer: D Explanation: Encryption is used to ensure the confidentiality of information. In this case you should make use of file level encryption. File level encryption is a form of disk encryption where individual files or directories are encrypted by the file system itself. This is in contrast to full disk encryption where the entire partition or disk, in which the file system resides, is encrypted.

QUESTION 267 Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future? A. Application firewalls B. Manual updates C. Firmware version control D. Encrypted TCP wrappers Answer: DE Explanation: Wrapping sensitive systems with a specific control is required when protecting data in transit. TCP wrappers are also security controls. TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or inetd query replies, to be used as tokens on which to filter for access control purposes. TCP Wrapper should not be considered a replacement for a properly configured firewall. Instead, TCP Wrapper should be used in conjunction with a firewall and other security enhancements in order to provide another layer of protection in the implementation of a security policy.

QUESTION 268 Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen? A. Hashing B. Screen locks C. Device

passwordD. Encryption Answer: DExplanation:Encryption is used to ensure the confidentiality of information. QUESTION 269 An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.Which of the following database designs provides the BEST security for the online store? A. Use encryption for the credential fields and hash the credit card fieldB. Encrypt the username and hash the passwordC. Hash the credential fields and use encryption for the credit card fieldD. Hash both the credential fields and the credit card field Answer: CExplanation:Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables. One main characteristic of hashing is that the algorithm must have few or no collisions ?in hashing two different inputs does not give the same output. Thus the credential fields should be hashed because anyone customer will have a unique credit card number/identity and since they will use their credit cards for many different transactions, the credit card field should be encrypted only, not hashed. QUESTION 270A system administrator has been instructed by the head of security to protect their data at-rest. Which of the following would provide the strongest protection? A. Prohibiting removable mediaB. Incorporating a full-disk encryption systemC. Biometric controls on data center entry pointsD. A host-based intrusion detection system Answer: B Explanation:Full disk encryption can be used to encrypt an entire volume with 128-bit encryption. When the entire volume is encrypted, the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption. This would be best to protect data that is at rest. QUESTION 271Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information? A. Employ encryption on all outbound emails containing confidential information.B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.C. Employ hashing on all outbound emails containing confidential information.D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention. Answer: AExplanation:Encryption is used to ensure the confidentiality of information and in this case the outbound email that contains the confidential information should be encrypted. QUESTION 272After recovering from a data breach in which customer data was lost, the legal team meets with the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.Which of the following controls support this goal? A. Contingency planningB. Encryption and stronger access controlC. Hashing and non-repudiationD. Redundancy and fault tolerance Answer: BExplanation:Encryption is used to protect data/contents/documents. Access control refers to controlling who accesses any data/contents/documents and to exercise authorized control to the accessing of that data. QUESTION 273A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered. Which of the following is occurring? A. The user is encrypting the data in the outgoing messages.B. The user is using steganography.C. The user is spamming to obfuscate the activity.D. The user is using hashing to embed data in the emails. Answer: BExplanation:Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message. QUESTION 274A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.Which of the following describes how the employee is leaking these secrets? A. Social engineeringB. SteganographyC. HashingD. Digital signatures Answer: BExplanation:Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message. QUESTION 275Which of the following functions provides an output which cannot be reversed and converts data into a string of characters? A. HashingB. Stream ciphersC. SteganographyD. Block ciphers Answer: AExplanation:Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way.it is not reversible. Incorrect Answers:B: A stream cipher is similar to a block cipher in that they are both symmetric methods of cryptography. The difference is that with a stream cipher the data is encrypted one bit, or byte, at a time whereas with a block cipher the algorithm works on chunks of data.C: Steganography is the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or

message and use that file to hide your message.D: A block cipher is a symmetric method in cryptography that encrypts data in chunks; very similar to stream ciphers. Latest SY0-401 questions and answers from CompTIA Exam Center offered by Lead2pass for free share now! Read and remember all real questions answers, Guarantee pass SY0-401 real test 100% or full money back! SY0-401 new questions on Google Drive: <https://drive.google.com/open?id=0B3Syig5i8gpDVzFZWEExUbFM0YU0> 2017 CompTIA **SY0-401** exam dumps (All 1868 Q&As) from Lead2pass: <https://www.lead2pass.com/sy0-401.html> [100% Exam Pass Guaranteed]