CHAPTER 30

Recovering from a Disaster

IN THIS CHAPTER

- Ongoing Backup and Recovery Preparedness
- When Disasters Strike
- Disaster Scenario Troubleshooting
- Recovering from a Server or System Failure
- Managing and Accessing Windows Server Backup Media
- Windows Server Backup Volume Recovery
- Recovering Role Services and Features

When organizations need to recover data or restore business services and operations after a disruption in business operations, having a well-formulated and validated recovery plan is vital to success. This requires a disciplined process of creating and maintaining backup and recovery procedures and documentation, as well as periodically validating the recovery tasks by simulating different failure scenarios and recovering data and applications.

In addition to having a disaster recovery plan, many organizations—not just the organizations that are required by law—should also implement and follow a strict change management system to evaluate the benefits and risks associated with proposed changes to current business systems, services, applications, and operational processes.

This chapter, as a complement to Chapter 29, "Backing Up the Windows Server 2016 Environment," details how to recover a Windows Server 2016 environment using Windows Server Backup after a failure or disaster has occurred. In addition to system recovery, this chapter provides some best practices and ideas organizations should consider when planning how to support and restore operation to the computer and network infrastructure when system failures and disasters occur.

Ongoing Backup and Recovery Preparedness

Creating and documenting processes that detail how to properly back up and recover from a disaster is an essential step in a disaster recovery project. Equally important as creating these processes is periodically reviewing, validating,

and updating the processes. Disaster recovery planning should not be considered a project for the current calendar year; instead, it should be considered an essential part of regular business operations and should have dedicated annual budget and assigned staff.

Each year, many businesses, business divisions, or departments update their computer and network infrastructure and change the way they provide services to their staff, vendors, and clients. In many of these cases, the responsible information technology staff, cross-departmental managers, executives, and employees are not involved or properly informed in advance of the execution or implementation of these changes. Computer and network infrastructure changes can have ripple effects throughout an entire organization during transition and during disaster and failure situations, so proper planning and approval of changes should always be performed and documented.

To reduce the risk of a change negatively impacting business operations, many organizations implement processes that require new projects and system changes to be submitted, evaluated, and either approved or rejected based on the information provided. Although this chapter does not focus or even really discuss project management, all organizations that utilize computer and network infrastructures should consider implementing a project management office and change-control committee to review and oversee organizational projects and infrastructure changes.

Project Management Office

Many organizations have introduced project management offices (PMOs) into their business operations. A PMO is used to provide somewhat of a project oversight committee to organizations that frequently operate several projects simultaneously. Organizations that utilize a proven project methodology can further extend this methodology to include workflow processes that include checkpoints with the PMO staff.

The role of the PMO can be different in almost every organization, but most include a few key functions. The role of the PMO usually involves reviewing proposed projects to determine how or if the project deliverables coincide with the organization's current or future business plans or strategies. PMO membership can also be very different among organizations. PMO membership can include departmental managers, directors or team leads, executive staff, employee advocates, and, in some cases, board members. Having the PMO staff represent views and insight from the different levels and departments of an organization enables the PMO to add value to any proposed project.

Having diverse staff included in the PMO staff enables the organization to evaluate and understand current and proposed projects and how these projects will positively or negatively affect the organization as a whole. General functions or roles a PMO can provide include the following:

- **High-level project visibility**—All proposed projects are presented to the PMO and if approved, the project is tracked by the PMO. This provides a single entity that is knowledgeable and informed about all ongoing and future projects in an organization and how they align to business and technical objectives.

- **Project sounding board**—When a new project is proposed or presented to the PMO, the project will be scrutinized and many questions will be asked. Some of these questions might not have been considered during the initial project design and planning phases. The PMO improves project quality by constantly reviewing and monitoring projects from when the project is proposed and during regular scheduled project status and PMO meetings.
- **Committee-based project approval or denial**—The PMO is informed of all the current and future projects as well as business direction and strategy and is the best-equipped group to decide on whether a project should be approved, denied, or postponed.
- **Enterprise project management**—The PMO tracks the status of all ongoing projects and upcoming projects, which enables the PMO to provide additional insight and direction with regard to internal resource utilization, vendor management for outsourced projects, and, of course, project budget and scheduling.

Change Control

Whereas a PMO improves project management and can provide the necessary checkpoints to verify that backup and recovery requirements are addressed within the new projects, an organization with a change-control system can ensure that any proposed changes have been carefully evaluated and scheduled before approval or change execution. Change control involves a submittal, review, and approval process for each change that typically includes the following information:

- **Change description**—Includes which systems will be changed, what the change is, and why it is proposed or required
- **Impact of the change**—Details if any systems or services will be unavailable during the execution of the change and who will be affected or impacted by the change
- **Change duration**—Details how long it will take to execute and complete the change and, if necessary, revert or roll back the change
- **Change schedule**—Includes the proposed date and time to execute the change
- **Change procedure**—Details how the change will be executed, including a detailed description; this usually also includes detailed steps or an accompanying document
- **Change rollback plan**—Details the steps necessary to recover or roll back the change in the event that the change causes undesirable results
- **Change owners**—Includes who will execute the change and is responsible for communicating the status and results of the change back to the change-control committee

A change-control committee, similar to a PMO, is made of up of managers, executives, and employee advocates who will review and determine if the change is approved, denied, or needs to be postponed. Proposed changes are submitted in advance. A day or two later,

a change-control review meeting is held where each change is discussed by the change-control committee and the change owner and the change will be approved, denied, postponed, or closed, or more information will be requested.

During failure or disaster situations, going through the normal change-control process might not be an option due to the impact of the failure. During these situations, emergency change-request processes should be followed. An emergency change request usually involves getting the particular departmental manager and the responsible information technology manager, director, or CIO to sign off on the change before it is executed. In short, all changes need to be considered and approved, even in failure scenarios when time is of the essence. When an administrator is troubleshooting and trying to resolve a failure or trying to recover from a disaster, especially in a stressful situation, making changes without getting approval can lead to costly mistakes. Following the proper change-control and emergency change-control processes to inform and involve others, getting approval from management, and following documented processes will provide accountability and might even save the administrator's job.

Disaster Recovery Delegation of Responsibilities

At this point, the organization might have a documented and functional backup and recovery plan, a PMO, and a change-control committee, but the ownership and maintenance of disaster recovery operations is not yet defined or assigned. Disaster recovery roles, functions, or responsibilities might be wrapped up into an existing executive's or manager's duties, or a dedicated staff member might be required. Commonly, disaster recovery responsibilities are owned by the chief information officer, operations manager, chief information security officer, or a combination of these positions. Of course, responsibilities for different aspects of the overall disaster recovery plan are delegated to managers, departmental leads, and staff volunteers as necessary. An example of delegating disaster recovery responsibilities is contained in the following list:

- The chief information officer is responsible for disaster recovery planning and maintaining and executing disaster recovery-related tasks for the entire telecom, desktop and server computer infrastructure, network infrastructure, and all other electronic and fax-related communication.
- The manager of facilities or operations is responsible for planning alternate office locations and offsite storage of original or duplicates of all important paper documents, such as leases, contracts, insurance policies, stock certificates, and so on, to support disaster recovery operations to alternate sites or offices.
- The manager of human resources is responsible for creating and maintaining emergency contact numbers for the entire company, storing this information offsite, and communicating with employees to provide direction and information prior to disasters striking and during a disaster recovery operation.

The list of responsibilities can be very granular and extensive, and disaster recovery planning should not be taken lightly or put on the back burner. Although there are many aspects of disaster recovery planning, the remainder of this chapter focuses only on the

disaster recovery responsibilities and tasks that should be assigned to qualified Windows administrators who need to support a Windows Server 2016 environment.

When Disasters Strike

When a failure occurs or disaster strikes is when not only having but also following a disaster recovery plan is most important. Having a procedure or checklist to follow allows all involved parties to be on the same page and understand what steps are being taken to rectify the situation. The following sections detail steps that can be followed to ensure that no time is wasted and that resources are not being led in the wrong direction.

Qualifying the Disaster or Failure

When a system failure occurs or is reported as failed, the information can come from a number of different sources and should be verified. The reported issue can be caused by user or operator error, network connectivity, or a problem with a specific user account configuration or status. A reported system failure should be verified as failed by performing the same steps reported by the reporting party.

If the system is, in fact, in a failed state, the impact of the failure should be noted, and this information should be escalated within the organization so that a formal recovery plan can be created. This can be known as qualifying the disaster or failure. An example of qualifying a failure includes a short description of the failure, the steps used to validate the failure, who is affected, how many end users are affected, which dependent applications or systems are affected, which branch offices are affected, and who is responsible for the maintenance and recovery of this system.

Validating Priorities

When a disaster strikes that affects an entire server room or office location, the priority of restoring systems and operations should already be determined. First and foremost are the core infrastructure systems, such as networking and power, followed by authentication systems, and the remaining core bare-minimum services. In the event of a failure that involves multiple systems (e.g., a web server failure that supports 10 separate applications), the priority of recovery should be presented and approved by management. If each of these 10 applications takes 30 minutes to recover, it could be 5 hours before the system is fully functional, but if one particular application is critical to business operations, this application should be recovered first. Always perform checkpoints and verification to ensure that the priorities of the organization are in line with the recovery work that is being performed.

Synchronizing with Business Owners

Prioritizing the recovery of critical and bare-minimum business systems is part of disaster recovery planning. When a situation strikes that requires an entire data center or group of systems to be restored or recovered, the steps that will be followed need to be put back in front of the business owners. Remember that between the time a disaster recovery plan is created and the time the failure occurs, business priorities might have shifted and the

business owners might be the only ones aware of this change. During a recovery situation, always take the time to stay calm and focused and communicate with the managers, executives, and business owners so that they can be informed of the progress. An informed business owner is less likely to stay in the server room or data center if he or she believes that recovery efforts are in good hands.

Communicating with Vendors and Staff

When a failure or a disaster strikes, communication is key. Regardless of whether customers, vendors, employees, or executives are affected, some level of communication is required or suggested. This is where the skills of an experienced manager, sales executive, technical consultant, and possibly even lawyers can be most valuable. Providing too much information, information that is too technical, or, worst of all, incorrect or no information is a common mistake technical staff frequently make. My recommendation to technical staff is to communicate only with your direct manager or his or her boss if you direct manager is unavailable. If the CEO or an end user asks for an update, try to defer to the manager as best you can so that focus can be kept on restoring services.

Assigning Tasks and Scheduling Resources

The situation is that we have a failure, we have an approved plan, we have communicated the situation, and we are ready to begin fixing the issue. The next step is to delegate the specific tasks to the qualified staff members for execution. As stated previously, hand off communication to a manager or spokesperson and only communicate through that person if possible. Determining who will restore a particular system is as important if not more important than assigning communication. Only certain technical staff members might be qualified to restore a system, so selecting the correct resource is essential.

When a serious failure has occurred, recovery efforts might require multiple technical resources onsite for an extended period of time. Furthermore, some dependencies might affect which systems can be restored, and, of course, the order or priority of restore will advance or delay the recovery of a system. Mapping out the extended recovery timeline and technical resource scheduling ensures that a technical resource is not onsite until their skills and time are required. Also, rotating technical resources after 6 to 8 hours of time helps to keep progress moving forward.

Recovering the Infrastructure

After the failure has been validated, the initial communications meetings have been held, restore tasks have been confirmed and possibly reprioritized, and recovery task assignment of resources has been completed, the recovery efforts can finally begin. Verify that each technical resource has all the documentation, phone numbers, software, and hardware they require to perform their task. Hold periodic checkpoint meetings, starting every 15 minutes and tapering off to every 30 or 60 minutes as recovery efforts continue.

Postmortem Meeting

After a system failure or disaster strikes, and the recovery has been completed, an organization should hold a meeting to review the entire process. The meeting might just be an event where individuals are recognized for their great work; however, the meeting will most likely involve reviewing what went wrong and identifying how the process could be improved in the future. A lot of interesting things will happen during disaster recovery situations—both unplanned and simulated—and this meeting can provide the catalyst for ongoing improvement of the processes and documentation.

Disaster Scenario Troubleshooting

This section of the chapter details the high-level steps that can be taken to recover from particular types of disaster scenarios, especially in Windows Server 2016 environments.

Network Outage

When an organization is faced with a network outage, the impact can affect a small set of users, an entire office, or the entire company. When a network outage occurs, the network administrators should perform the following tasks:

- Test the reported outage to verify if the issue is related to a wide-area network (WAN) connection between the organization and the Internet service provider (ISP), the router, a network switch, a firewall, a physical fiber or copper network connection or network port, or line power to any of the aforementioned devices.
- After the issue is isolated or, at least, the scope of the issue is understood, the network administrator should communicate the outage to the necessary managers or business owners and, as necessary, open communication to outside support vendors and ISP contacts to report the issue and create a trouble ticket. And no, this should not go out in email if the network is down.
- Create a logical action plan to resolve the issue and execute the plan.
- Create and distribute a summary of the cause and result of the issue and how it can be avoided in the future. Close the trouble ticket as required.

Physical Site Failure

In the event a physical site or office cannot be accessed, a number of business operations might be suspended. Planning how to mitigate issues related to physical site limitations can be extensive, but should include the considerations discussed in the following sections.

Physical Site Access Is Limited but Site Is Functional

This section lists a few considerations for a situation where the site or office cannot be accessed physically, but all systems are functional:

- Can the main and most critical phone lines be accessed or forwarded remotely?

- Is there a remote-access solution to allow employees with or without notebooks/laptop computers to connect to the organization's network and perform their work?
- Are any other business operations that require onsite access tied to a service-level agreement, such as responding to paper faxes or submitted customer support emails, phone calls, or custom applications?

Physical Site Is Offline and Inaccessible

This section lists a few considerations for a situation where the resources in a site are nonfunctional. This scenario assumes that the site resources cannot be accessed across the network or Internet, and the datacenter is offline with no chance of a quick recovery. When planning for a scenario such as this, the following items should be considered:

- Can all services be restored in an alternate capacity—or at least the most critical systems, such as the main phone lines, fax lines, devices, applications, system, and remote access services?
- If systems are cut over to an alternate location, what is the impact in performance, or what percentage of end-user load can the system support?
- If systems are cut over to an alternate location, will there be any data loss or will only some data be accessible?
- If the decision to cut over to the alternate location is made, how long will it take to cut over and restore the critical services?
- If the site outage is caused by power loss or network issues, how long of an outage should be sustained before deciding to cut over services to an alternate location?
- When the original system is restored, if possible, what will it take to failback or cut the systems back to the main location, and is there any data loss or synchronization of data involved?

These short lists merely break the surface when it comes to the planning of or dealing with a physical site outage, but, hopefully, they will spark some dialogue in the disaster recovery planning process to lead the organization to the solution that meets their needs and budget.

Server or System Failure

When a server or system failure occurs, administrators must decide on which recovery plan of action will be the most effective. Depending on the particular system, in some cases, it might be more efficient to build a new system and restore the functionality or data. In other cases, where rebuilding a system can take several hours, it might be more prudent to troubleshoot and repair the problem.

Application or Service Failure

If a Windows Server 2016 system is still operational but a particular application or service on the system is nonfunctional, in most cases troubleshooting and attempting repair or

restoring the system to a previous backup state is the correct plan of action. The Windows Server 2016 event log is useful and it should be one of the first places an administrator looks to determine the cause of a validated issue. Following troubleshooting or recovery procedures for the particular application is the next logical step. For example, if an end user deleted a folder from a network share, the preferred recovery method might be to use shadow copy backups to restore the data instead of the Windows Server Backup.

For Windows services, using Server Manager to review the status of the role and role services assists administrators in identifying and isolating problems because the Server Manager tool displays a filtered representation of Event Viewer items and service state for each role installed on the system. Figure 30.1 details that the File and Storage Services role FILESERVER1 had logged and issue related to the role service.

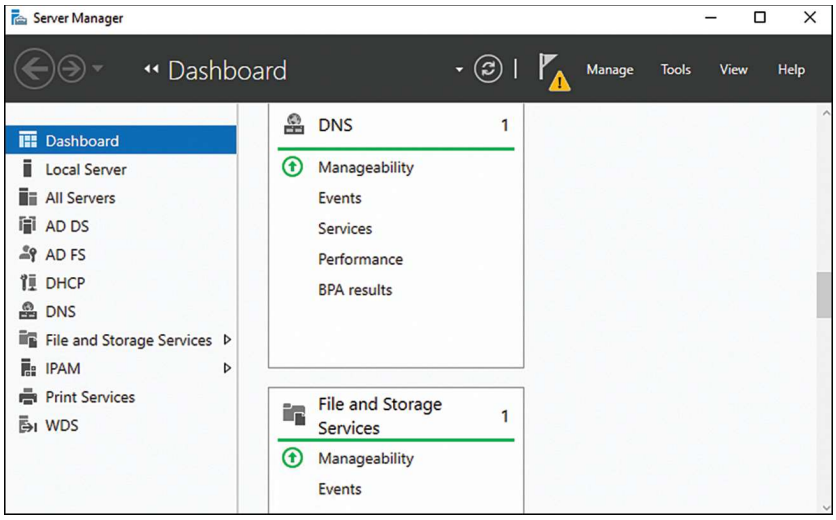

FIGURE 30.1 File and Storage Services role status.

Data Corruption or Loss

When a report has been logged that the data on a server is missing, is corrupted, or has been overwritten, Windows Server 2016 administrators have a few options to deal with this situation. Previous versions backed up with shadow copies can be used to restore selected files or folders, or Windows Server Backup can be used to restore the data. Using shadow copy backups, administrators and end users with the correct permissions can restore data right from the network. Using the restore features of Windows Server Backup, administrators can place the restored data back into the same folder by overwriting the existing data or placing a copy of the data with a different name based on the backup schedule date and time. For example, to restore a file named ClientProprosal.docx that was backed up on 6-10-2016 at 10:30 p.m., Windows Server Backup will restore the file as 2016-06-10 22-30 Copy of ClientProposal.docx.

Hardware Failure

When hardware failure occurs, a number of issues and symptoms might result. The most common issues related to hardware failures include system crashes, services or drivers stopping unexpectedly, frozen (hung) systems, and systems that are in a constant reboot cycle. When hardware is suspected as failed or failing on a Windows Server 2016 system, administrators should first review the event logs for any related system or application event warnings and errors. If nothing apparent is logged, hardware manufacturers usually provide several different diagnostic utilities that can be used to test and verify hardware configuration and functional state. Don't wait to call Microsoft and involve their professional support services department as they can be working in conjunction with your team to capture and review debugging data.

When a system is suspected of having hardware issues and it is a business-critical system, steps should be taken to migrate services or applications hosted on that system to an alternate production system, or the system should be recovered to new hardware. Windows Server 2016 can tolerate a System Image Recovery to alternate hardware if the system is an exact or close hardware match with regard to the motherboard, processors, hard disk controller, and network card. Even if the hardware is exact and the disk arrays, disk IDs, and volume or partition numbers do not match, a System Image Recovery to alternate hardware might fail if no additional steps are taken during the restore or recovery process.

Recovering from a Server or System Failure

When a failure or issue is reported regarding a Windows Server 2016 system, the responsible administrator should first perform the standard validation tests to verify that there is a real issue. The following sections include basic troubleshooting steps when failure reports are based around data or application access issues, network issues, data corruption, or recovery issues.

Access Issues

When end users report issues accessing a Windows Server 2016 system but the system is still online, this is categorized as an access issue. Administrators should start troubleshooting access issues by first verifying that the system can be accessed from the system console and then verify that it can be accessed across the network. After that is validated, the access issue should be tested to reveal whether the access issue is affecting everyone or just a set of users. Access issues can be system or network related, but they can also be related to security configurations on the network or local system firewall or application, share, or NTFS permissions. The following sections can be used to help troubleshoot access issues.

Network Access Troubleshooting

Troubleshooting access to a system that is network related can involve the networking group as well as the Windows Server 2016 system administrators. When networking issues are suspected, the protocol and system IP information should be noted before any tests are performed. Tests should be performed from the Windows system console to determine whether the system can access other devices on the local network and systems on neighboring networks located across a gateway or router. Tests should be performed using both

the system domain name system (DNS) names as well as IP addresses and, if necessary, IPv6 addresses.

If the system can communicate out but users still cannot access the system, possible causes could be an incorrect IP subnet mask, default gateway or routing table, or firewall restrictions imposed locally or through group policy. Windows Firewall is enabled by default on Windows Server 2016 systems, and the firewall supports multiple firewall profiles simultaneously if multiple adapters are installed on the system. If a network is identified incorrectly as a public network instead of a private or domain network, depending on the firewall profile settings, this may undesirably restrict access. When administrators follow the proper procedures for installing roles and role services, during role installation, exceptions will be added to the firewall. Administrators can review the settings using the Windows Firewall applet from Control Panel, but to get very detailed firewall information, the Windows Firewall with Advanced Security console should be used. You can access this console through the Server Manager Tools menu.

Share and NTFS Permissions Troubleshooting

If network connectivity and firewall configurations check out, the next step in troubleshooting access issues is to validate the configured permissions to the affected application, service, or shared folder. For application access troubleshooting, see the section "Application Access Troubleshooting" and the application vendors' administration and troubleshooting guides. For Windows services and share folder permission troubleshooting, the Event Viewer can assist tremendously, especially if auditing is enabled. Auditing can be enabled within an Active Directory group policy on the Windows Server 2016 local computer policy, but auditing must also be enabled on the particular NTFS folder. For information about local and domain group policies, see Chapter 25, "Group Policy Management for Network Clients." To troubleshoot share and NTFS permissions, review the following sections.

Validating Share and NTFS Permissions

When you need to validate share and NTFS permissions, you can do so in several ways. The preferred method is to use the File and Storage Services node within Server Manager, as detailed in the following steps:

1. Log on to the Windows Server 2016 system with an account with administrator privileges and open Server Manager from the taskbar.
2. Click the File and Storage Services link in the tree pane on the left.
3. In the File and Storage Services section of Server Manager, click the Shares link and in the Shares pane, right-click the desired share, and select Properties.
4. Select the Permissions link on the left, and the window will display the NTFS permission and will summarize the share permissions.
5. Click the Customize Permissions button.
6. In the Advanced Security Settings window, select the permission tab for NTFS permissions, the Share tab for share permissions, and the Central Policy tab to review Dynamic Access Control settings for the shared folder, as shown in Figure 30.2.

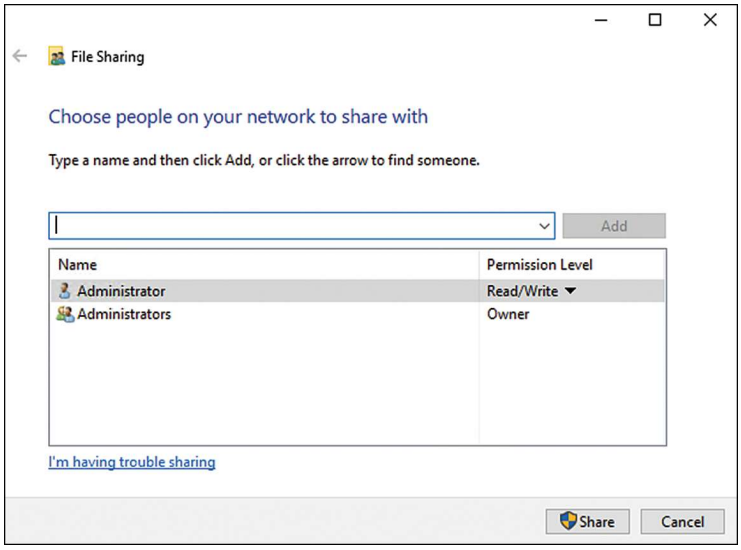

FIGURE 30.2 Reviewing shared folder permissions.

7. Close the Advanced Security Settings window, close the share properties window, and close Server Manager when done reviewing the settings.

Enabling Auditing for NTFS Folders

Enabling auditing on an NTFS folder can be a helpful aid in troubleshooting access to server folders. Enabling auditing for NTFS folders is a two-part configuration involving either Group Policy or local computer policy audit settings as well as configuring auditing on the folder itself. To enable auditing for a folder on a Windows Server 2016 system, follow these steps:

1. Log on to the Windows Server 2016 system with an account with administrator privileges and open Server Manager.
2. From the Server Manager tools menu, select Local Security Policy.
3. In the tree pane of the Local Security Policy window, double-click Local Policies, and double-click Audit Policy.
4. In the tasks pane, double-click Audit Object Access.
5. When the Audit Object Access window opens, check the Failure check box, and click OK, as shown in Figure 30.3.

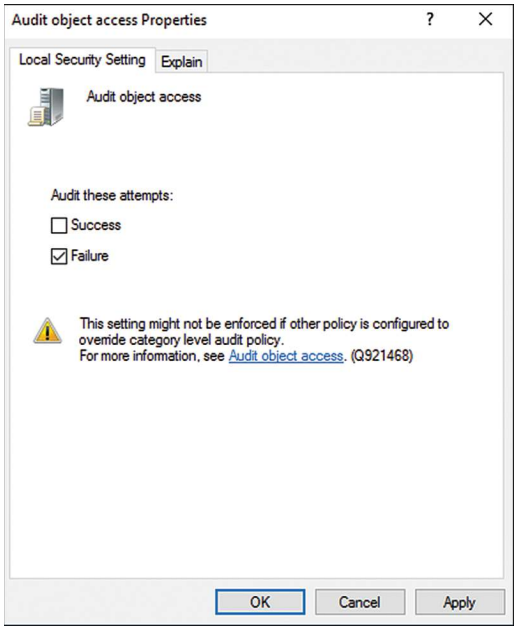

FIGURE 30.3 Enabling failure audit for object access.

6. Close the Local Security Policy window.
7. Back in Server Manager, click the File and Storage Services link in the tree pane on the left.
8. In the File and Storage Services section of Server Manager, click the Shares link and in the Shares pane, right-click the desired share, and select Properties.
9. Select the Permissions link on the left, and the window will display the NTFS permission and will summarize the share permissions.
10. Click the Customize Permissions button.
11. Select the Auditing tab and click the Add button to change the audit settings of the shared folder. In this particular example, we want to log failed attempts to access the folder, so we will use the Everyone group and enable All Failure Audits.
12. In the Audit Entry for the share window, click the Select a Principal link at the top of the window.
13. When the Select User, Computer, Service Account, or Group window opens, type in **Everyone** and click OK.
14. In the Auditing Entry for the share window, pull down the Type menu and select the Fail Audit option and check the Full Control Permissions check box. Click OK to apply the new audit settings, as shown in Figure 30.4.

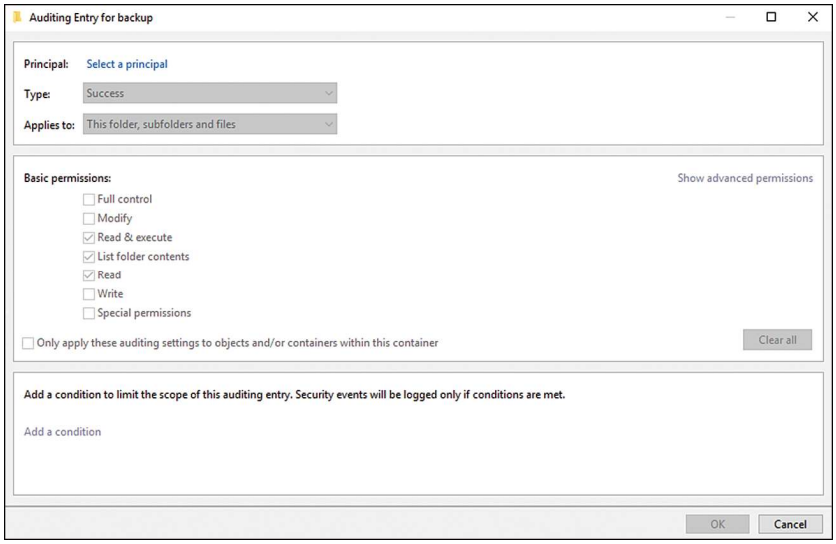

FIGURE 30.4 Configuring an audit entry for the shared NTFS folder.

15. In the Advanced Security Settings window, check the Replace All Existing Inheritable Auditing Entries check box, and then click OK.
16. Click OK to close the Advanced Security page, click OK to close the share property pages, and close Server Manager.

When a user then attempts to access the shared folder with the enabled audit settings and fails based on permissions, a failed audit entry will be logged on the server's Security event log.

Application Access Troubleshooting

If the issue revolves around an application running on a Windows Server 2016 system, troubleshooting the application according to the application administration guide is the recommended approach. Many applications can be configured to use authentication using Active Directory via Lightweight Directory Access Protocol (LDAP), Kerberos, or NTLM authentication. Also, applications might use custom application or database user accounts and might still require permissions via application pool identities and service accounts. Each application is different and should be treated as such. Specific troubleshooting guides and backup and recovery documentation should be created for applications before they are deployed on a network.

Data Corruption and File and Folder Recovery

When data is reported as corrupted or deleted, administrators have the option of restoring the data from backup using Windows Server Backup or from a previous version of that folder captured with shadow copies. When data has been mistakenly changed, overwritten, or deleted, the only options are to recover from shadow copies or from backup media as detailed in the following sections.

Recovering File and Folder Data Using Shadow Copies

To recover individual files and folders using previously created shadow copies, follow these steps:

1. Log on to a Windows Server 2016 system or a client system running Windows XP SP1 or greater and open Windows Explorer.
2. In the Windows Explorer window type **\\servername** and press Enter, where servername represents the NetBIOS or fully qualified domain name of the server hosting the file share. The share must already exist and be stored on a volume in which a shadow copy has already been created.
3. Right-click the folder beneath the share, or the share itself, that contains the file or folder that will be restored, and select Restore Previous Versions.
4. When the window opens, if necessary, select the Previous Versions tab, and select the desired previous version based on the date and click Open, as shown in Figure 30.5.

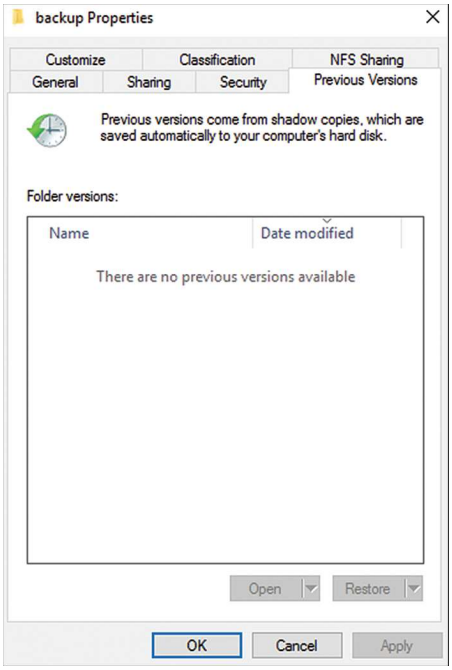

FIGURE 30.5 Selecting the desired previous version shadow copy for data restore.

5. After the previous version of the share or folder beneath the share is opened, displaying the contents, select a single file single folder or multiple items, right-click the selections, and choose Copy. This places the selected items in the Clipboard.
6. Close the previous version window and close the share or folder properties window.

7. Browse to the location where the data will be restored, right-click in an empty location, and choose Paste. Overwrite the file as desired or restore the data to an alternate location, and close all the windows when completed.

Recovering File and Folder Data Using Windows Server Backup

To recover individual files and folders using backup media created with Windows Server Backup, follow these steps:

1. Log on to the Windows Server 2016 system with an account with administrator privileges and open Server Manager from the taskbar.
2. From the Tools menu, select Windows Server Backup.
3. When the Windows Server Backup window opens, select Local Backup in the tree pane.
4. Click Recover from the actions pane.
5. On the Getting Started page, select either to restore data previously backed up from the local computer or a different computer. For this example, select This Server (Servername), and click Next to continue.
6. On the Select Backup Data page, select the date of the backup by selecting the correct month and click the particular day.
7. After the month and day are selected, if multiple backups were run in a single day, click the Time drop-down list arrow, and select the correct backup. Click Next to continue after the month, day, and time are selected.
8. On the Select Recovery Type page, select the Files and Folders option button, and click Next to continue.
9. On the Select Items to Recover page, expand the server node; select the disks, folders, and files to be restored; and click Next to continue.

NOTE

Unlike other backup utilities, Windows Server Backup does not contain check boxes to select items for recovery. To select an item or multiple items, simply click the item to highlight it and use the Shift or Ctrl keys to make multiple sections.

10. On the Specify Recovery Options page, specify whether the files will be restored to the original location or an alternate location. Do not click Next.
11. On the Specify Recovery Options page, if the restore will be placed in the original location, specify how to deal with existing files by choosing to either create copies in the same folder, overwrite the existing data with restore data or do not recover items that already exist. Also check or uncheck the check box to determine whether NTFS access control lists will also be restored with the data.

12. On the Confirmation page, verify the restore selections and options. If everything is correct, click the Recover button to start the recovery process.
13. On the Recovery Progress page, verify the success of the recovery or troubleshoot the errors if the recovery fails.
14. Click Close to complete the recovery and close Windows Server Backup.
15. Browse to the location of the restore to verify the recovery and notice that there are two copies, the original and the restored, which is named after the date and time the backup was taken. When you have finished, log off of the server.

Managing and Accessing Windows Server Backup Media

Windows Server Backup for Windows Server 2016 can create backups of the entire system, specific volumes, system state, applications or granular folders or files. Windows Server Backup also supports the exclusion of individual files and folders within a configured backup job. Windows Server Backup can store backups on dedicated locally attached disk folders, dedicated backup disks or network shared folders. New for Windows Server 2016 there is also an online cloud-based backup that can backup data volumes directly to the cloud with the use of a specific online backup agent.

Windows Server Backup can be configured to run a scheduled backup or a manual backup. Either can be run from the graphical user interface or the command-line utility, but the backup options, including where the backup can be stored and the recovery options available, are different.

Windows Server Backup Dedicated Disks

Windows Server Backup can be used to run a manual backup or it can be used to run a scheduled backup. Scheduled backups can be stored on locally attached disks that are dedicated to Windows Server Backup, a folder on a local volume or a network shared folder. When a scheduled Windows Server Backup job is created, the administrator can define which locally attached disks, folder or network share will be used to store the backups. During the creation of the scheduled job, if dedicated disk are selected, which are recommended, the allocated disks will each be repartitioned and reformatted. Windows Server Backup stamps the disk volume to match the time and date the scheduled job is created. By default, this disk is available only on the local system and only through the Windows Server Backup program.

A Windows Server Backup disk can have a drive letter added after the initial backup is created if the disk needs to be accessed from within the operating system, from across the network, or if the backup data needs to be copied to additional disks or network folders for offsite storage. Backups contained on a Windows Server Backup dedicated disk can be used to restore an entire system, an entire volume, a set of specified files and folders, or application data.

Network Shared Folders

When Windows Server Backup is configured to back up to a network shared folder, backup administrators need to consider a few things. First, the share and NTFS permissions should be configured so that only backup administrators and specific service accounts can access and read this data. Also, if this share contains data that will be replicated by a third-party provider, special permissions may need to added to support this. Another very important point to note about network shared folders for Windows Server Backup is that only the most recent copy of the backup will be stored, because each backup overwrites the previous. This is unlike backup to dedicated disks, which can store multiple versions and copies of a Windows Server 2016 system backup.

Windows Server Backup Volume Recovery

When an entire disk or disk volume has been corrupted and needs to be recovered, you can use Windows Server Backup to restore the volume. Local disks, local folder backups, and network shared folder backups can be used to restore an entire volume using Windows Server Backup. When an entire volume needs to be recovered, unless the volume contains system data, the volume can be restored using the Windows Server Backup program from within a running operating system. If the volume contains system folders, the restore needs to be restored using the Repair Your Computer option when booting the system using the Windows installation media.

Windows Server 2016 Data Volume Recovery

When a data volume on a Windows Server 2016 system has failed and needs to be restored using Windows Server Backup, follow these steps:

1. Log on to the Windows Server 2016 system with an account with administrator privileges and open Server Manager from the taskbar.
2. From the Tools menu, select Windows Server Backup.
3. When the Windows Server Backup window opens, select Local Backup in the tree pane.
4. Click Recover from the actions pane.
5. On the Getting Started page, select either to restore data previously backed up from the local computer or a different computer. For this example, select This Server (Servername), and click Next to continue.
6. On the Select Backup Data page, select the date of the backup by selecting the correct month and click the particular day.
7. After the month and day are selected, if multiple backups were run in a single day, click the Time drop-down list arrow, and select the correct backup. Click Next to continue after the month, day, and time are selected.
8. On the Select Recovery Type page, select the Volumes option button, and click Next to continue.

9. On the Select Volumes page, the window displays each of the volumes contained in the backup that was previously chosen. Check the box next to the desired volume that will be restored, and select the destination volume to which you will restore the backed-up volume. Click Next to continue after the correct selections are made.
10. After clicking Next on the Select Volumes page, a window opens requesting confirmation that the data on the volumes will be lost by the recovery process; click Yes to continue with the volume recovery process.
11. On the Confirmation page, review the selections. If everything looks correct, click the Recover button to start the volume recovery.
12. On the Recovery Progress page, the recovery status of the volume will be displayed. After the recovery completes, review the results and click Close if the recovery was successful; otherwise, select the Errors tab to review the errors.
13. If the volume recovery was successful, the only additional step that might be required is to reboot the system if the data on the volume is shared or used by any applications or services. Reboot as required.

Windows Server 2016 System Volume Recovery

You cannot restore a system volume by using Windows Server Backup. System volumes can only be restored using the Windows installation recovery environment from the Windows installation media. System volumes should only be restored separately when the system volume is corrupted or failed but the system hardware has not changed and data disks remain intact. Any Windows disk that contains system volumes will be erased and restored as part of this process. If a single disk contains two volumes (the system volume and a separate data volume), the data volume will also be erased and restored by this process. To restore the system volume, follow these steps:

1. Boot your system using the Windows Server 2016 installation media. If necessary, configure the BIOS to allow booting from the CD/DVD drive and, if prompted, press a key to boot from the DVD.
2. When the Windows Setup interface opens, select the correct language, time, and keyboard settings, and click Next to continue.
3. On the next page, click the Repair Your Computer link located in the lower-left corner of the window.
4. On the Choose an Option page, select the Troubleshoot tile.
5. On the Advanced Options page, select System Image Recovery tile to continue.
6. On the System Image Recovery page, select to restore the Windows Server 2016 installation by clicking the tile.
7. A Re-Image Your Computer window will open and will display the option to restore the latest available system image by default.

8. On the Choose Additional Restore Options page, the box labeled Only Restore System Drives will be checked and dimmed (grayed out). Do not make any other changes. Click Next to continue. This will leave any other disks intact, but any volumes that are hosted on the same disks that contain system volumes will be formatted, re-created, and restored as well.
9. The next page details the date and time of the backup that will be restored, the server that will be restored, and the volumes that are contained in this restore set. Review the information and click Finish to continue with the recovery of the system volumes.
10. A dialog box will appear stating that all drives selected will be restored with the data in the system image. Click Yes to approve this and continue.

    The recovery time frame will vary depending on the size of the system volume, the performance of the volume, and the restore disk or network share. After the recovery completes, the system will automatically reboot.
11. After the system reboots, log on and verify functionality. If everything is back up and running, run a full backup and log off.

Windows System Image Recovery

In the event of a complete system failure, it might be necessary to restore a Windows Server 2016 system in its entirety. If this is the case, perform the same steps as a system volume recovery, except on the Choose Additional Restore Options page, check the Format And Repartition Disks check box. This restores all the disks and also performs the disk partitioning, drive letter assignment, and mounted volume configuration. If different-size disks are provided, the restore partitions the disks based on the original size of the disk volumes only. Smaller disks will cause the restore to fail, but larger disks can easily be extended after the recovery completes successfully.

Recovering Role Services and Features

Each particular role on a Windows Server 2016 system can have very specific backup and recovery procedures. As a general rule, though, performing full backups using Windows 2016 Windows Server Backup will enable the restore of a system to a previous imaged version, including restoring all Windows Server roles, role services, features, and configuration to that previously backed-up state. Most role services can be restored using a system-state recovery; however, a system-state recovery cannot be restored in part; only the complete system state can be restored. Depending on the role, however, with Windows 2016, different application databases, such as the cluster database, can be restored separately as long as a compatible Volume Shadow Copy writer was installed and functional before the backup was taken.

Windows Server 2016 System-State Recovery

When operating systems become corrupt or unstable or a role service needs to be rolled back to a previously backed-up state, the quickest and easiest way to perform this task is to restore the system state. The system state can be backed up independently, but is also contained within a full server backup. To restore the System state on a member server from a previous backup, follow these steps:

1. Log on to the Windows Server 2016 system with an account with administrator privileges and open Server Manager from the taskbar.
2. From the Tools menu, select Windows Server Backup.
3. When the Windows Server Backup window opens, select Local Backup in the tree pane.
4. Click Recover from the actions pane.
5. On the Getting Started page, select either to restore data previously backed up from the local computer or a different computer. For this example, select This Server (Servername), and click Next to continue.
6. On the Select Backup Data page, select the date of the backup by selecting the correct month and click the particular day.
7. After the month and day are selected, if multiple backups were run in a single day, click the Time drop-down list arrow, and select the correct backup. Click Next to continue after the month, day, and time are selected.
8. On the Select Recovery Type page, select the System-State option button, and click Next to continue.
9. On the Select Location for System-State Recovery page, click the Original Location button and click Next to continue. If this system was a domain controller, more options will be available, but that is covered later in this chapter.
10. On the Confirmation page, review the section and then press Recover to start the process. Once the process starts a checkbox to Automatically reboot the server to complete the recovery process is presented and already checked by default.
11. After the system reboots, log on to the server to verify functionality. If the system is working properly, perform a full system backup.

Active Directory Recycle Bin Recovery

Let me start this section with a very clear statement: If you need to recover a deleted Active Directory object and the Active Directory Recycle Bin was not enabled before the object was deleted, skip this section and proceed to the following "Active Directory Authoritative Restore" section. If the Active Directory Recycle Bin feature was enabled before an Active Directory object was deleted, follow these steps to recover objects using the Active Directory Recycle Bin:

1. Log on to the Windows Server 2016 domain controller system with an account with domain administrator privileges and open Server Manager from the taskbar.
2. From the Tools menu of Server Manager, select Active Directory Administrative Center.
3. In the tree pane, click the domain to reveal each of the root-level organizational units and containers. Select the Deleted Objects container.
4. In the center pane, each of the deleted objects should be listed. Review or expand the Last Known Parent column. This is the location the object will be restored to by default.
5. If the last known parent is where the object should be restored to, right-click the object and select Restore, as shown in Figure 30.6. If the object should be restored elsewhere, right-click the object and select Restore To, and then select the desired container or organizational unit.

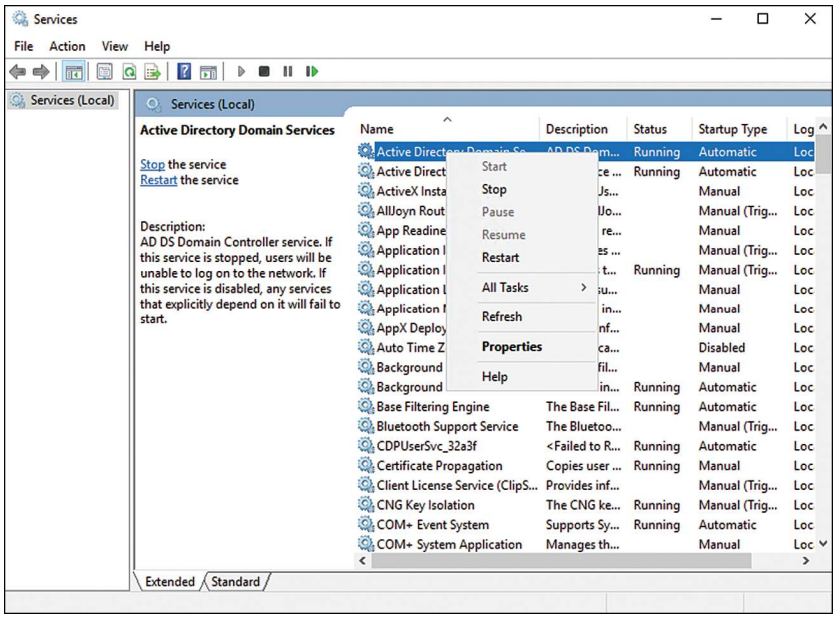

FIGURE 30.6 Restoring a deleted Active Directory user object from the AD Recycle Bin.

System-State Recovery for Domain Controllers

Performing a system-state recovery for a domain controller is similar to the recovery of a member server, but the domain controller will need to be booted into Directory Services Restore Mode (DSRM) before attempting the restore. Recovering the system state of a domain controller should only be performed if one or more of the following scenarios are encountered:

- A deleted object needs to be restored and the Active Directory Recycle Bin is not enabled, or was not enabled when the object was originally deleted.
- The Active Directory Domain Services service will not start or the Active Directory database on that domain controller is corrupted.
- The files, possibly including scripts or group policies, stored in the SYSVOL folder have been deleted or overwritten and need to be restored and replicated across the domain.

Before a domain controller can be booted into DSRM, the DSRM password is required. This password is configured when a system is promoted to a domain controller and is stored locally on each domain controller. The DSRM username is administrator with no domain designation, and the password can manually be changed on a working domain controller by using Ntdsutil. To restore the system state of a domain controller, follow these steps:

1. If the domain controller is still functional, log on to the Windows Server 2016 domain controller system with an account with domain administrator privileges.
2. Click the charms bar and select the Search option. In the Search pane, type in **MSConfig** and press Enter.
3. In the MSConfig.exe window (System Configuration Utility), select the Boot tab.
4. In the Boot Options section, check the Safe Boot check box, click the Active Directory Repair button, as shown in Figure 30.7, and then click OK.
5. The System Configuration utility will ask for a reboot, and if there are no additional tasks to perform, click the Restart button to boot the system into DSRM.

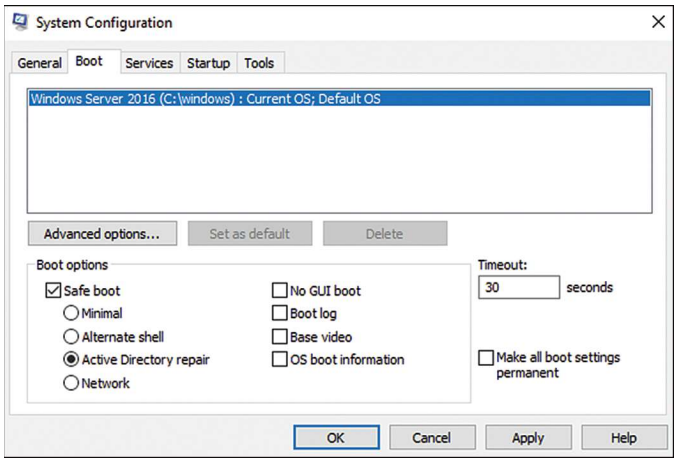

FIGURE 30.7 Using the System Configuration utility to boot a domain controller into Directory Services Restore Mode.

6. When the system completes a reboot, log on as administrator with the DSRM password. Make sure to specify the local server as the logon domain (e.g., DC\administrator instead of companyabc\administrator).
7. Open Server Manager from the taskbar, and from the Tools menu select Windows Server Backup.
8. When the Windows Server Backup window opens, select Local Backup in the tree pane.
9. Click Recover from the actions pane.
10. On the Getting Started page, select either to restore data previously backed up from the local computer or a different computer. For this example, select This Server (Servername), and click Next to continue.
11. On the Select Backup Data page, select the date of the backup by selecting the correct month and click the particular day.
12. After the month and day are selected, if multiple backups were run in a single day, click the Time drop-down list arrow, and select the correct backup. Click Next to continue after the month, day, and time are selected.
13. On the Select Recovery Type page, click the System-State button, and click Next to continue.
14. On the Select Location for System-State Recovery page, click the Original Location button. Do not check the Perform an Authoritative Restore of Active Directory Files box unless the SYSVOL folder and contents will be marked as the definitive/authoritative copy and replicated to all other domain controllers. For our example, we will recover the system state but not mark the SYSVOL as an authoritative restore, as shown in Figure 30.8. Click Next to continue.

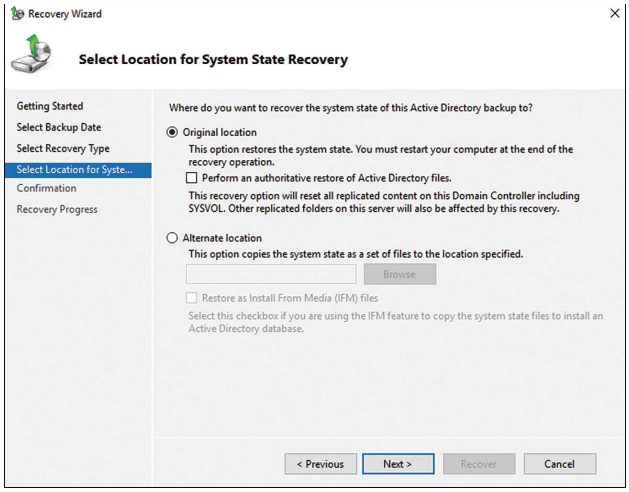

FIGURE 30.8 Restoring a domain controller system state without marking the SYSVOL data as authoritative.

15. A dialog box opens that states that this recovery option will cause the server to re-sychronize after recovery. Click OK to continue.
16. On the Confirmation page, verify that the system state is listed, and click Recover to start the system-state recovery of the domain controller.
17. A dialog box opens detailed that once the recovery is started it cannot be paused and a restart will be required to complete the recovery. Click Yes to start the recovery. System-state recovery can take a long time to complete, so be patient.
18. When the system-state restore completes, Windows Server Backup presents a dialog box with only a Restart button and no other option. Restart the server now.
19. When the server reboots, it reboots into DSRM again. Log on with the DSRM local username and password.
20. Once logged in, a wbadmin command prompt will open stating that the restore completed successfully. Close the command prompt window by pressing Enter.
21. Click the charms bar and select the Search option. In the Search pane, type in **MSConfig** and press Enter.
22. In the MSConfig.exe window (System Configuration Utility), select the Boot tab.
23. In the Boot Options section, uncheck the Safe Boot check box, and then click OK.
24. If an authoritative restore of Active Directory objects is not required, click the Restart button in the dialog box and allow the server to reboot normally. If an authoritative restore is required, click the Exit Without Restart button in the dialog box and perform the steps outlined in the following section, "Active Directory Authoritative Restore."

Active Directory Authoritative Restore

When Active Directory has been modified and needs to be restored to a previous state, and this rollback needs to be replicated to all domain controllers in the domain and possibly the forest, an authoritative restore of Active Directory is required. An authoritative restore of Active Directory can include the entire Active Directory database, a single object, or a container, such as an organizational unit, including all objects previously stored within the container. When performing an authoritative restore of a container or a single object within Active Directory, run the system-state restore of a domain controller as previously outlined and after the first reboot continue with these steps:

1. Open a command prompt on the domain controller that is running in DSRM and has just completed a system-state recovery and a reboot.
2. In the command prompt window, type **Ntdsutil** and press Enter.
3. Type **Activate Instance NTDS** and press Enter.
4. Type in **Authoritative Restore** and press Enter.

5. To restore a single object, type **Restore Object** followed by the distinguished name of the previously deleted object. For example, to restore an object named Jamil Droubi in the Users container of the companyabc.com domain, type the following:

```
Restore Object "cn=Jamil Droubi,cn=users,
dc=companyabc,dc=com"
```

6. To restore a container or organizational unit and all objects beneath it, replace the "restore object" with "restore subtree," followed by the appropriate distinguished name.
7. After the appropriate command is typed in, press Enter. A window opens asking for confirmation of the authoritative restore; click the Yes button to complete the authoritative restore of the object or subtree.
8. The Ntdsutil tool displays the name of the text file that may contain any back-links for objects just restored. Note the name of the files and whether any back-links were contained in the restored objects.
9. Type **quit** and press Enter; type **quit** again to close out of the Ntdsutil tool. Type **exit** to close the command prompt window.
10. Open the charms bar and select the Settings icon and click the Power button.
11. Choose to restart the server and select Operating System Recovery(Planned) as the reason, and then click Continue to restart the server into normal operation.
12. After normal reboot, verify the authoritatively restored object replicates to all domain controllers, and then perform a full backup of the domain controller.

Restoring the SYSVOL Folder

When a domain controller system state is restored, the SYSVOL is also restored to the point in time the backup was taken. If the SYSVOL that has replicated across the domain needs to be rolled back, an authoritative restore of the SYSVOL, known previously as a primary restore of SYSVOL, must be performed. To perform an authoritative restore of the SYSVOL, restore the system state of a domain controller using Windows Server Backup, as outlined in the earlier in the "System-State Recovery for Domain Controllers" section, but on the Select Location for System-State Recovery page, check the Perform an Authoritative Restore of Active Directory Files check box. Follow the steps to recover the system state of the domain controller, and then boot the domain controller normally. When the domain controller is returned to operation, the Active Directory database syncs with other domain controllers, but the SYSVOL of this particular domain controller is pushed out to all other domain controllers in the domain as the authoritative copy and overwrites the other copies. No other steps are required.

Restoring Group Policies

When group policies need to be restored, performing a restore of the SYSVOL as well as the Active Directory database is required. Group Policy object information is stored in a container in the domain naming context partition called the Group Policy Objects

container, and the files are stored in the SYSVOL folder on each domain controller. The most effective way to back up and restore group policies is to use the backup and restore features built in to the Group Policy Management Console included with Windows Server 2016 Group Policy Management Tools. For detailed information about how to back up and recover group policies using the Group Policy Management Console, see Chapter 18, "Windows Server 2016 Group Policies and Policy Management."

Summary

This chapter covered many aspects Windows Server 2016 recovery. Administrators and IT managers responsible for disaster recovery tasks, including planning and execution, should test all plans regularly to ensure that in the event of a failure, the critical systems and most important data are backed up and can be recovered properly and efficiently.

Many technologies and solutions built in to Windows Server 2016 were covered in this chapter to provide you with useful recovery processes for Windows Server Backup or shadow copies to recover data and systems. Also covered were the tasks involved in creating the recovery plan, testing it, and making sure (through tested procedures) that what you think will happen in a recovery process actually can happen.

Best Practices

The following are best practices from this chapter:

- Document all backup and recovery procedures.
- Periodically test the restore procedures to verify accuracy and test the backup media to ensure that data can actually be recovered.
- Validate reported system failures before attempting to restore data or fix an issue.
- Allocate the appropriate hardware devices, including servers with enough processing power and disk space to accommodate the restored machines' resources.
- Store a copy of all disaster recovery documentation and copies of dedicated Windows Server Backup disks at secure offsite locations.
- Understand the dependencies of the applications and services to the operating system to choose whether to rebuild or restore from backup.
- Identify and document special restore requirements for each server.
- If an organization has not or cannot standardize on server hardware platforms or if systems will be used in production even when the hardware is at its end of life or the maintenance on a system has expired; consider moving critical physical systems to virtual servers.
- When planning for recovery scenarios, ensure that a proper chain of communication is established to allow the technical staff to focus on their tasks and not be inundated with requests for status updates.