

System Admin

| | |
|-------------------------|--|
| Active Directory | <p>Active Directory is a Directory Service created by Microsoft. Active Directory provides a centralized control for network administration and security. Active Directory stores all information and settings for a deployment in a central database, and allows administrators to assign policies.</p> <p>Active Directory is primarily used to store directory objects like users and groups and computers printers.</p> <p>Using Active Directory brings a number of advantages to your network:-</p> <ul style="list-style-type: none">Centralized user account managementCentralized policy management (group policy)Better security management <p>Where is the AD database held? What other folders are related to AD?</p> <p>The AD data base is store in c:\windows\ntds\NTDS.DIT.</p> <p>What is the use of SYSVOL folder</p> <p>All active directory data base security related information store in SYSVOL folder and it's only created on NTFS partition.</p> <p>Active Directory Database files:</p> <ul style="list-style-type: none">All AD changes didn't write directly to NTDS.DIT database file, first write to EDB.Log and from log file to database, EDB.Che used to track the database update from log file, to know what changes are copied to database file. <ol style="list-style-type: none">1. NTDS.DIT NTDS.DIT is the AD database and store all AD objects, Default location is the %system root%\ntds\ntds.dit, Active Directory database engine is the extensible storage engine which us based on the Jet database2. EDB.Log EDB.Log is the transaction log file when EDB.Log is full, it is renamed to EDB Num.log where num is the increasing number starting from 1, like EDB1.Log3. EDB.Che EDB.Che is the checkpoint file used to trace the data not yet written to database file this indicate the starting point from which data is to be recovered from the log file in case if failure.4. Res1.log & Res2.log Res is reserved transaction log file which provide the transaction log file enough time to shutdown if the disk didn't have enough space. |
|-------------------------|--|

| | |
|-----------------------|---|
| | <p>What are the requirements for installing AD on a new server?</p> <ol style="list-style-type: none"> 1 The Domain structure. 2 The Domain Name. 3 Storage location of the database and log file. 4 Location of the shared system volume folder. 5 DNS configuration. <p>Define DSRM Mode?</p> <p>Directory Services Restore Mode (DSRM) is a special boot mode for repairing or recovering Active Directory. It is used to log on to the computer when Active Directory has failed or needs to be restored.</p> <p>To manually boot in Directory Services Restore Mode, press the F8 key repeatedly. Do this immediately after BIOS POST screen, before the Windows logo appears. (Timing can be tricky; if the Windows logo appears you waited too long.) A text menu will appear. Use the up/down arrow keys to select Directory Services Restore Mode or DS Restore Mode. Then press the Enter key.</p> <p>What is global catalog?</p> <p>The Global Catalog is a database that contains all of the information pertaining to objects within all domains in the Active Directory environment</p> <p>What is the difference between local, global and universal groups?</p> <p>Domain local groups assign access permissions to global domain groups for local domain resources.</p> <p>Global groups provide access to resources in other trusted domains. Universal groups grant access to resources in all trusted domains.</p> <p>What is group nesting?</p> <p>Adding one group as a member of another group is called 'group nesting'. This will help for easy administration and reduced replication traffic</p> <p>What is Forest?</p> <p>A collection of one or more Active Directory domains that share a common schema, configuration, and global catalog.</p> <p>What is tree?</p> <p>An Active Directory tree is a collection of Active Directory domains that begins at a single root and branches out into peripheral, child domains. Domains in an Active Directory tree share the same namespace. An Active Directory forest is a collection of Active Directory trees, similar to a real world forest. Catalog Server.</p> |
| AD Replication | <p>Below is a command to replicate from a specified DC to all other DC's.</p> <p>Repadmin /syncall DC_name /APed</p> <p>All partitions, Push, Enterprise cross sites, Distinguished names</p> <p>C:\Users\Administrator>repadmin /syncall /AdeP</p> |

| | |
|---|--|
| | <p>To check replication status</p> <p>C:\Users\Administrator>Repadmin /replsummary</p> |
| AD Sites | <p>A site can simply be defined as a physical location or network. It can be separate building, separate city or even in separate country.</p> <p>Sites in Active Directory represent the physical structure of well-connected network.</p> <p>Benefits :</p> <p>Creating AD sites benefits you in several ways, the first of which is that creating these sites lets you control replication traffic over WAN links.</p> <p>Two types of replication:</p> <p>Intra-site replication, which occurs between DCs that are members of the same site.</p> <p>Inter-site replication, which occurs between DCs at different sites.</p> <p>Purpose of AD Sites :</p> <p>Primarily, the purpose of AD Sites is to control replication.</p> <p>Secondarily, it is used for administration (for example, GPOs and GPP targeting can apply per site).</p> |
| Operational roles for DC (Domain controller) and ADC (Additional Domain Controller) | <p>1. Operational roles for DC (Domain controller) are:</p> <p>Domain Naming Master</p> <p>Schema Master</p> <p>RID Master</p> <p>PDC Emulator</p> <p>Infrastructure Master</p> <p>2. Operational roles for ADC (Additional Domain Controller) are:</p> <p>PDC Emulator</p> <p>RID Master</p> <p>Infrastructure Master</p> |
| Main Difference Between Windows server 2008 and 2012 | <p>1) New Server Manager: Create, Manage Server Groups</p> <p>2) Hyper-V Replication: The Hyper-V Replica feature allows you to replicate a virtual machine from one location to another with Hyper-V and a network connection—and without any shared storage required. This is a big deal in the Microsoft world for disaster recovery, high availability and more. VMware does this, too, but the vendor charges new licensees extra for the capability.</p> <p>3) Expanded PowerShell Capabilities</p> <p>4) IIS 8.0 and IIS 7 in 2008</p> <p>5) Hyper-V 3.0</p> <p>6) PowerShell 3.0</p> |

| | |
|---|--|
| OU? | OU means for Organizational Unit. It is a container within Active Directory which can hold users, groups and computers. It is the smallest unit on which administrator can assign group policy settings. |
| What is a Domain? | A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database. A tree can have multiple domains. |
| Domain Controller? | <p>A domain controller (DC) or network domain controller is a Windows-based computer system that is used for storing user account data in a central database.</p> <p>It is the centerpiece of the Windows Active Directory service that authenticates users, stores user account information and enforces security policy for a Windows domain.</p> <p>Domain controller allows system administrators to grant or deny users access to system resources, such as printers, documents, folders, network locations, etc., via a single username and password.</p> |
| Group Policy? | <p>Group Policy is a feature of the Microsoft Windows NT family of operating systems that control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.</p> <p>Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory service containers: sites, domains, or organizational units (OUs).</p> <p>Where are group policies stored? C:\Windows\System32\GroupPolicy.</p> |
| What are GPOs (Group Policy Objects)? | <p>A Group Policy Object (GPO) is a collection of settings that control the working environment of user accounts and computer accounts. GPOs define registry-based policies, security options, software installation and maintenance options, script options, and folder redirection options.</p> <p>There are two kinds of Group Policy objects:</p> <ul style="list-style-type: none"> • Local Group Policy objects are stored on individual computers. • Nonlocal Group Policy objects, which are stored on a domain controller, are available only in an Active Directory environment. |
| Few benefits of using GPMC. | <p>Easy administration of all GPOs across the entire Active Directory Forest</p> <p>View of all GPOs in one single list</p> <p>Backup and restore of GPOs Migration of GPOs across different domains and forest.</p> |
| How frequently is the client policy refreshed? | 90 minutes give or take. |
| LDAP? | LDAP (Light-Weight Directory Access Protocol) determines how an object in an Active Directory should be named. LDAP is the industry standard directory access protocol, making Active Directory widely accessible to management and query applications. Active Directory supports LDAPv2 and LDAPv3. |

| | |
|--|---|
| <p>What is DNS?</p> | <p>Domain Name System, DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember.</p> <p>Two types of lookup in DNS: Forward lookup: it converts Domain name to IP address. Reverse lookup: it converts IP address to Domain name.</p> <p>Three types of zone: Primary zone Secondary zone Stub zone</p> <p>Protocol : UDP Port number : 53</p> |
| <p>What are main Email Servers and which are their ports?</p> | <p>Email servers can be of two types: Incoming Mail Server (POP3, IMAP, HTTP) The incoming mail server is the server associated with an email address account. There cannot be more than one incoming mail server for an email account. In order to download your emails, you must have the correct settings configured in your email client program.</p> <p>Outgoing Mail Server (SMTP) Most outgoing mail servers use SMTP (Simple Mail Transfer Protocol) for sending emails. The outgoing mail server can belong to your ISP or to the server where you setup your email account.</p> <p>The main email ports are:</p> <ul style="list-style-type: none"> • POP3 – port 110 • IMAP – port 143 • SMTP – port 25 • HTTP – port 80 • Secure SMTP (SSMTP) – port 465 • Secure IMAP (IMAP4-SSL) – port 585 • IMAP4 over SSL (IMAPS) – port 993 • Secure POP3 (SSL-POP) – port 995 |
| <p>What do Forests, Trees, and Domains mean?</p> | <p>Forests, trees, and domains are the logical divisions in an Active Directory network.</p> <p>A domain is defined as a logical group of network objects (computers, users, devices) that share the same active directory database.</p> <p>A tree is a collection of one or more domains and domain trees in a contiguous namespace linked in a transitive trust hierarchy.</p> |

| | |
|--|--|
| | At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible. |
| Why do we use DHCP? | Dynamic Host Configuration Protocol assigns dynamic IP addresses to network devices allowing them to have a different IP address each time they are connected to the network. |
| How DHCP work? | <p>DHCP Stands for Dynamic host configuration protocol.</p> <p>DHCP is a protocol used for automatic configuration IP address in client computers connected to IP networks. DHCP operates on a client server model in four phases.</p> <p>Discover: A client broadcasts DHCP Discover message when it comes alive on the network.</p> <p>Offer: When a DHCP server receives the DHCP Discover message from the client, it reserves an I P address for the client and sends a DHCP Offer message to the client offering the reserved IP address.</p> <p>Request: The client receives the DHCP offer message and broadcasts a DHCP request message to show its consent to accept the offered IP address.</p> <p>Acknowledge: When the DHCP server receives the DHCP Request message from the client, it sends a DHCP Ack packet to the client. At this point the IP configuration process is complete.</p> |
| What is DHCP Scope? | A range of IP address that the DHCP server can assign to clients that are on one subnet. |
| What protocol and port does DHCP use? | UDP protocol and 67 port in client and 68 port in server. |
| What is a DHCP lease? | A DHCP lease is the amount of time that the DHCP server grants to the DHCP client permission to use a particular IP address. A typical server allows its administrator to set the lease time. |
| DHCP Database location? | C:\WINDOWS\System32\DHCP directory. |
| Define Dora Process & why it is used? | Discover, Offer, request and acknowledgement. it is used to assign ip address automatically to client systems. |
| What are Lingering Objects? | <p>A lingering object is a deleted AD object that still remains on the restored domain controller in its local copy of Active Directory. They can occur when changes are made to directories after system backups are created.</p> <p>When restoring a backup file, Active Directory generally requires that the backup file be no more than 180 days old. This can happen if, after the backup was made, the object was deleted on another DC more than 180 days ago.</p> |

| | |
|---|---|
| How can we remove Linger Objects? | Windows Server 2003 and 2008 have the ability to manually remove lingering objects using the console utility command REPADMIN.EXE. |
| What is LDAP? Why it is used? | LDAP is the Lightweight Directory Access Protocol. Its an active directory protocol, Basically, it's a protocol used to access data from a database. |
| Why should you not restore a DC that was backed up 6 months ago? | When restoring a backup file, Active Directory generally requires that the backup file be no more than 180 days old. If you attempt to restore a backup that is expired, you may face problems due to lingering objects. |
| What is nslookup? | Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through Control Panel. |
| PTR record? | This program record is used to check if the server name is connected with the IP address, it is exactly opposite to the A record. This record is basically created in reverse lookup zone, so it is also known as Reverse DNS records or pointer record. PTR record= Give me an IP address and I will give you the name |
| What is AAA? | AAA stands for authentication, authorization and accounting, used to control user's rights to access network resources and to keep track of the activity of users over a network. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS). |
| What is loop back? | Loopback address is 127.0.0.1, An address that sends outgoing signals back to the same computer for testing. |
| What is wins server? | Windows Internet Name Service (WINS) servers dynamically map IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address. |
| What is MBR? | Short form Master Boot Record, a small program that is executed when a computer boots up. Typically, the MBR resides on the first sector of the hard disk. The program begins the boot process by looking up the partition table to determine which partition to use for booting. |
| What happens when we type URL in browser? | First the computer looks up the destination host. If it exists in local DNS cache, it uses that information. Otherwise, DNS querying is performed until the IP address is found. |
| What is SCSI? | SCSI stands for Small Computer System Interface. It is a standard electronic interface that allows personal computers to communicate with peripheral hardware such as disk drives, tape drives, printers, CD-ROM drives. In SCSI the rate of data transmission is fast. SCSI Hard Disk Speed R.P.M. is fast in SCSI Data Transmission speed is 320 MBPS in the Network. In SCSI Controller We can connect Maximum 15 physical devices in the system. |
| BSOD | A Blue Screen error is mainly due to hardware or software incompatibility within the system. The most common reasons for a Blue Screen of Death (BSD) are unwanted software installation, high CPU usage and faulty RAM. |

| | |
|--|--|
| Differentiate Between NTFS & FAT? | <p>NTFS is the current file system used by Windows. It offers features like security permissions (to limit other users' access to folders), quotas (so one user can't fill up the disk), shadowing (backing up) and many other features that help Windows.</p> <p>FAT32 is the older Microsoft filesystem, primarily used by the Windows 9X line and Windows could be installed on a FAT32 partition up to XP. In comparison, FAT32 offers none of what was mentioned above, and also has a maximum FILE (not folder) size of 4GB, which is kind of small these days, especially in regards to HD video.</p> |
| Antivirus | The prime job of an antivirus is protect your system from computer viruses. Your computer may be standalone or part of network or connected to Internet you need an antivirus program. It actively monitors when you are using your system for any virus threat from different sources. If it found one it tries to clean or quarantine the virus ultimately keeping your system and data safe. |
| Does a windows administrator have to be critical? | Yes and I can explain how. A system administrator is responsible for an entire network which means he/she must take care of multiple things in the same time which is not an easy task. In order to achieve this, an administrator must have high organization skills and a high technical knowledge and he/she must prevent the problems from happening so that he/she won't have to be forced to fix them. |
| Is it possible for a computer to be able to browse the internet without having a default gateway? | Yes it is as long as we use a public IP address. The gateway is required as a router or firewall when using an intranet address. |
| In how much time are the security changes applied on the domain controllers? | Including policies for personal and public lockout, the changes apply immediately. The changes also include passwords and LSA or Local Security Authority. |
| Where is the storage place of the environmental settings and documents from the roaming profile? | These documents and settings are deposited locally until the user's log off, when they are moved into the shared folder from the server so the log on at a fresh system may take a while because of this. |
| Domain Functional Level Forest Functional Level | <p>To find the Domain Functional Level, use this command: Get-ADDomain fl Name,DomainMode</p> <p>To find the Forest Functional Level, use this command: Get-ADForest fl Name,ForestMode</p> |
| Fault tolerance | Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of some (one or more faults within) of its components. |
| RAID | <p>RAID LEVEL 0</p> <p>Following are the key points to remember for RAID level 0.</p> <ul style="list-style-type: none"> ▪ Minimum 2 disks. |

| | |
|--|--|
| | <ul style="list-style-type: none"> ▪ Excellent performance (as blocks are striped). ▪ No redundancy (no mirror, no parity). ▪ Don't use this for any critical system. <p>RAID LEVEL 1</p> <p>Following are the key points to remember for RAID level 1.</p> <ul style="list-style-type: none"> ▪ Minimum 2 disks. ▪ Good performance (no striping. no parity). ▪ Excellent redundancy (as blocks are mirrored). <p>RAID LEVEL 5</p> <p>Following are the key points to remember for RAID level 5.</p> <ul style="list-style-type: none"> ▪ Minimum 3 disks. ▪ Good performance (as blocks are striped). ▪ Good redundancy (distributed parity). ▪ Best cost effective option providing both performance and redundancy. Use this for DB that is heavily read oriented. Write operations will be slow. <p>RAID LEVEL 10</p> <p>Following are the key points to remember for RAID level 10.</p> <ul style="list-style-type: none"> ▪ Minimum 4 disks. ▪ This is also called as "stripe of mirrors" ▪ Excellent redundancy (as blocks are mirrored) ▪ Excellent performance (as blocks are striped) ▪ If you can afford the dollar, this is the BEST option for any mission critical applications (especially databases). |
| Windows Server 2012, 2012 r2 and 2016 | <p>2012</p> <p>Some of the new features introduced in Server 2012 are</p> <ul style="list-style-type: none"> ▪ Hyper-V ▪ IP Address Management ▪ New Windows Task Manager ▪ Metro style start menu <p>2012r2</p> <ul style="list-style-type: none"> ▪ Improvements in VM & Storage ▪ Windows Server essential role ▪ Hyper-V improvements in replication, migration etc. <p>2016</p> <ul style="list-style-type: none"> ▪ Nano Server -> No GUI & headless version of windows server. |

| | |
|---|---|
| | <ul style="list-style-type: none"> ▪ Hyper Containers -> Provides enhanced isolation ▪ Docker Support -> Use to manage window server & Hyper-V containers. ▪ Rolling upgrades for Hyper-V & storage cluster ▪ Nested Virtualization -> Can run Hyper-V within Hyper-V ▪ PowerShell direct <p>PowerShell Direct is a new feature that enables to open a PowerShell session from a Hyper-V host to its virtual machines without using the networking. Using this feature, we can automate the network configuration and almost everything for the virtual machine deployment.</p> <ul style="list-style-type: none"> ▪ Secure boot -> Linux secure boot for VM's |
| Recovering Active Directory | <p>We can recover AD from server backup.</p> <p>Press F8 key and Boot into Directory Services Restore Mode (DSRM) and perform a System State restore to restore the Active Directory (AD) database.</p> |
| Difference between Authoritative and Non-Authoritative restore of Active Directory | <p>Non-Authoritative:- Non-Authoritative method will restore an active directory to the server in which the restore is being done and will then receive all of the recent updates from its replication partners in the domain.</p> <p>Authoritative: - Authoritative method restores the DC directory to the state that it was in when the backup was made, then overwrites all the other DC's to match the restored DC.</p> |
| Performing a non-authoritative restoration | <ul style="list-style-type: none"> ▪ The easiest way to complete this process is to stop the Active Directory Domain Services and then restore a valid system state. ▪ To stop the Active Directory Domain Services you will need to open an elevated command prompt and then enter the following command: <p>Net Stop NTDS</p> <ul style="list-style-type: none"> ▪ Shutting down the Active Directory Domain Services causes several other dependency services to stop as well. The dependency services that are affected by this operation include: <p>Kerberos Key Distribution Center Intersite Messaging DNS Server DFS Replication</p> <ul style="list-style-type: none"> ▪ Once the Active Directory Domain Services have been stopped, you can restore a System State backup. When the restoration process completes, you will likely be prompted to reboot your server. You should avoid rebooting because doing so will cause the Active Directory Domain Services to be restarted, which will cause your restoration to be overwritten. |

| | |
|---|--|
| |  <pre> C:\Users\Administrator>net stop ntds The following services are dependent on the Active Directory Domain Services. Stopping the Active Directory Domain Services service will also stop the ces. Kerberos Key Distribution Center Intersite Messaging DNS Server DFS Replication Do you want to continue this operation? (Y/N) [N]: y The Kerberos Key Distribution Center service was stopped successfully. The Intersite Messaging service is stopping. The Intersite Messaging service was stopped successfully. The DNS Server service is stopping. The DNS Server service was stopped successfully. . The DFS Replication service was stopped successfully. The Active Directory Domain Services service is stopping. The Active Directory Domain Services service was stopped successfully. C:\Users\Administrator> </pre> <ul style="list-style-type: none"> Restart the Active Directory Domain Services <p>Net Start NTDS</p> |
| <p>Performing an authoritative restore</p> | <ul style="list-style-type: none"> You can begin the process by entering the following commands: <p>Ntdsutil</p> <p>Activate Instance NTDS</p> <p>Authoritative Restore</p> <p>It allows you to validate that you are about to perform an authoritative restore within the correct Active Directory partition, as shown in Figure.</p>  <pre> Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved. C:\Users\Administrator>ntdsutil ntdsutil: activate instance nt ds Active instance set to "ntds". ntdsutil: authoritative restore authoritative restore: List NC CRs Opening DIT database... Done. Listing locally instantiated writeable partitions and associated cross-refs: 1) Partition: DC=DomainDnsZones,DC=lab,DC=com cross-ref: CN=42b5d0f3-256e-48fb-b556-f7b2e8fc0e7f,CN=Partitions,CN=Con figuration,DC=lab,DC=com 2) Partition: DC=ForestDnsZones,DC=lab,DC=com cross-ref: CN=b1563a5b-0baa-4732-b7af-e0412a156980,CN=Partitions,CN=Con figuration,DC=lab,DC=com 3) Partition: CN=Configuration,DC=lab,DC=com cross-ref: CN=Enterprise Configuration,CN=Partitions,CN=Configuration,D C=lab,DC=com 4) Partition: CN=Schema,CN=Configuration,DC=lab,DC=com cross-ref: CN=Enterprise Schema,CN=Partitions,CN=Configuration,DC=lab,D C=com 5) Partition: DC=lab,DC=com cross-ref: CN=LAB,CN=Partitions,CN=Configuration,DC=lab,DC=com Done. authoritative restore: _ </pre> <p>Now it's time to specify the object that needs to be restored. You can do so by using the Restore Object command. For example, suppose that you wanted to restore a user account named User1 that existed in the Users container in a domain named Contoso.com. To perform such a restoration, you would use the following command:</p> <p>Restore Object "CN=User1,CN=Users,DC=Contoso,DC=com"</p> |

| | |
|--|--|
| | <ul style="list-style-type: none"> Restart the Active Directory Domain Services Net Start NTDS |
|--|--|

FSMO

FSMO Roles – Flexible Single Master Operation is the main features of windows Active Directory server. Generally AD is a multi-master distributed database and these roles are used to reduce conflict and facilitate communication concerning replication between domain controllers

FSMO Roles are used for performing certain critical operations and it has to be performed very carefully, since tiny changes in these roles will result in the major issues of the active directory environment.

Generally FSMO roles are classified as 2 categories.

- **Forest Wide Roles (Forest Level)**
- **Domain Wide Roles (Domain Level)**

Since the operations are performed on Forest basis and domain basis these classifications has been made for the better understanding.

The detailed information about FSMO roles are as follows.

There are 5 FSMO roles in an Active Directory since the operations performed on forest level are classified as Forest Wide Roles and Domain based are Domain wide roles.

Forest Wide Roles:

These roles are applicable at the Forest level

- **Schema Master**
- **Domain Naming Master**

Domain Wide Roles:

These roles are applicable at the Domain level

- **RID Master**
- **PDC Emulator**
- **Infrastructure Master**

FSMO roles are one of the important interview questions for the Techies and I have seen in so many forums about the same, hence this topic is for the beginners.

By default all roles are assigned to first domain controller.

Schema Master:

- The schema master domain controller controls all the access related to updates and modifications to the schema.
- For the Entire Forest there can be only one Schema Master.
- Ensures updates are replicated to all the Domain Controller in the forest.
- In order to make changes or Updates on the schema level you must have access to the schema and you must be member of **Schema Administrators Group**.
- By default, the first server in the forest has Schema Master Role

Domain Naming Master:

- Domain Naming Master allows the additions or removals of Domains in the Forest
- For the Entire Forest there can be only one Domain Naming Master
- In order to make changes or Updates on the Domain Naming Master you must be member of **Enterprise Administrators Group**.
- By default, the first server in the forest has the domain naming master role

Relative Identifier Master:

- The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain.
- The RID Master manages the Security Identifier (SID) for every object within the particular domain
- Whenever a domain controller creates a new, user, group, organization Unit (OU) or computer object, it assigns the object a unique security ID (SID)
- By default, the first server in the domain is the RID Operations Master
- In order to change or move the RID Master role to another Server, you must be a member of **Domain Administrators Group**

PDC Emulator:

- The key role of PDC Emulator is act as a central manager for password Changes. It processes password changes from clients and replicates updates to the BDCs
- It also acts a central manager for Replication and Account Lockouts.
- Handles time synchronization
- At any time, there can be only one domain controller acting as the PDC emulator master in each domain in the forest.
- By default, the first server in the domain has PDC Emulator Master Role.
- In order to change or move the PDC Emulator role to another Server, you must be a member of **Domain Administrators Group**

Infrastructure Master Role:

- The infrastructure master compares its data with that of a global catalog
- Manages users and group references for objects between domains
- It Queries the global catalog server to ensure that references are current and updated.
- There is one infrastructure operations master in every domain in a forest.
- By default, it is placed in the first domain controller in the domain.
- In order to change or move the Infrastructure Master role to another Server, you must be a member of **Domain Administrators Group**.

Now will see about, How to find out which server has FSMO Roles

There are four ways to identify the FSMO roles, but here I am using the easy and cool one and that too using single command.

```
C:\Users\Administrator>netdom query fsmo
Schema master           DoubtsClearAD.doubtsclear.com
Domain naming master    DoubtsClearAD.doubtsclear.com
PDC                     DoubtsClearAD.doubtsclear.com
RID pool manager        DoubtsClearAD.doubtsclear.com
Infrastructure master    DoubtsClearAD.doubtsclear.com
The command completed successfully.
```

Scavenging:-

To remove the outdated DNS records from the DNS zone automatically, you should enable Scavenging through Zone properties. Scavenging will help you clean up old unused records in DNS.

DNS Zones:-

DNS Zones store DNS resource record information. Some common DNS records include:

A Record: Name to IP address mapping

CNAME: Maps an alias to the canonical name

MX Record: Used to identify mail servers

NS Record: Identifies the name servers for a particular zone

SOA: Start of Authority records

TXT: Allows any text to be inserted into a DNS record

Active Directory Integrated Zones:-

Active Directory Integrated Zones stores its zone data in Active Directory. Integrated zones can be replicated to all domain controllers in the domain and forest. Active Directory integrated zones use multi-master replication, this means any domain controller running the DNS server service can write updates to the zone for which they are authoritative.

Advantages of Active Directory integrated Zones

- Replication is faster, more secure and efficient.
- Better redundancy due to zone data being copied to all Domain Controllers
- Improved Security if secure dynamic update is enabled
- No need to schedule or manage zone transfers

What is ADFS?

Active Directory Federation Services (ADFS) is a Single Sign-On (SSO) solution created by Microsoft. As a component of Windows Server operating systems, it provides users with authenticated access to applications that are not capable of using Integrated Windows Authentication (IWA) through Active Directory (AD).

Developed to provide flexibility, ADFS gives organizations the ability to control their employees' accounts while simplifying the user experience: employees only need to remember a single set of credentials to access multiple applications through SSO.

How to reset the Directory Services Restore Mode (DSRM) password on a domain controller? What tool should you use?

To reset the DSRM password on a single domain controller, you should use ntdsutil utility. You can use Ntdsutil.exe to reset this password for the server on which you are working, or for another domain controller in the domain. Type ntdsutil and at the ntdsutil command prompt, type set dsrm password.

Types of Active Directory Groups:

There are two types of AD groups

Active Directory Security Groups - This type of group is used to provide access to resources. For example, you want to grant a specific group access to files on a shared folder. To do this, you need to create a security group.

Active Directory Distribution Groups - This type of group is used to create email distribution lists (usually used in Microsoft Exchange Server). An e-mail sent to such a group will reach all users in the group. This type of group cannot be used to provide access to domain resources, because they are not security enabled.

For each type of group, there are three group scopes:

Domain local - Used to manage access permissions to resources (files, folders and other types of resources) only in the domain where it was created.

Global - This group type can be used to provide access to resources in the another domain.

Universal - It is recommended to use it in big Active Directory forests.

A Domain Controller called ABC is failing replication with XYZ. How do you troubleshoot the issue?

Active Directory replication issue can occur due to variety of reasons. For example, DNS issue, network problems, security issues etc. Troubleshooting can start by verifying DNS records. Then remove and recreate Domain Controller replication link. Check the time settings on both replication partners.

Tell me few uses of NTDSUTIL commands?

We can use ntdsutil commands to perform database maintenance of AD DS, manage and control single master operations, Active Directory Backup restoration and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.

What is REPLMON?

The Microsoft definition of the Replmon tool is as follows; This GUI tool enables administrators to view the low-level status of Active Directory replication, force synchronization between domain controllers, view the topology in a graphical format, and monitor the status and performance of domain controller replication.

What is NETDOM ?

NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

Why do we need Netlogon?

Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services, and the domain controller cannot register DNS records.

Mention what are the components of AD?

Components of AD includes

Logical Structure: Trees, Forest, Domains and OU

Physical Structures: Domain controller and Sites

Mention what are lingering objects?

Lingering objects can exists if a domain controller does not replicate for an interval of time that is longer than the tombstone lifetime (TSL).

Mention what is TOMBSTONE lifetime?

Tombstone lifetime in an Active Directory determines how long a deleted object is retained in Active Directory. The deleted objects in Active Directory is stored in a special object referred as TOMBSTONE. Usually, windows will use a 60- day tombstone lifetime if time is not set in the forest configuration.

Mention what is the difference between domain admin groups and enterprise admins group in AD?

Enterprise Admin Group

Members of this group have complete control of all domains in the forest. By default, this group belongs to the administrators group on all domain controllers in the forest. As such this group has full control of the forest, add users with caution.

Domain Admin Group

Members of this group have complete control of the domain By default, this group is a member of the administrators group on all domain controllers, workstations and member servers at the time they are linked to the domain. As such the group has full control in the domain, add users with caution

What is SYSVOL, and why is it important?

SYSVOL is a folder that exists on all domain controllers. It is the repository for all of the active directory files. It stores all the important elements of the Active Directory group policy. The File Replication Service or FRS allows the replication of the SYSVOL folder among domain controllers. Logon scripts and policies are delivered to each domain user via SYSVOL. SYSVOL stores all of the security related information of the AD.

How would you manage trust relationships from the command prompt?

Netdom.exe is another program within Active Directory that allows administrators to manage the Active Directory. Netdom.exe is a command line application that allows administrators to manage trust relationship within Active Directory from the command prompt. Netdom.exe allows for batch management of trusts. It allows administrators to join computers to domains. The application also allows administrators to verify trusts and secure Active Directory channels.

Administering Active Directory Objects with PowerShell

| | |
|--|---|
| Create new AD User | New-ADUser User01 |
| Create new AD User with password | \$Password = ConvertTo-SecureString -String "Pass!23" -AsPlainText -Force New-ADUser -name User01 -Department IT -Title Manager -AccountPassword \$Password -Enabled \$true |
| Get AD User details | Get-ADUser User01 Get-ADUser -Identity User01 Get-ADUser -Identity User01 -Properties department, title |
| Get AD Users with filter | Get-ADUser -Filter {name -like "c*"} |
| Get inactive AD Users with filter | Get-ADUser -Filter {name -like "c*" -and enabled -eq "FALSE"} |
| Remove AD User | Remove-ADUser -Identity User01 |
| Create multiple AD Users | \$Password = ConvertTo-SecureString -String "Pass!23" -AsPlainText -Force 1..10 ForEach-Object {New-ADUser -Name "User\$PSItem" -AccountPassword \$Password -Enabled \$true} |
| Disable/Enable/Unlock AD Account | Disable-ADAccount -Identity User01 Enable-ADAccount -Identity User01 Unlock-ADAccount -Identity User01 |
| Last account logon | get-aduser -filter * -Properties lastlogondate ft name,lastlogondate |
| Last password reset | get-aduser -filter * -Properties lastlogondate,passwordlastset ft name,lastlogondate,passwordlastset |
| Disabled Accounts | Search-ADAccount -AccountDisabled -usersonly fl name |
| Locked out accounts | Search-ADAccount -LockedOut -UsersOnly fl name |
| Search AD Account | Search-ADAccount -PasswordNeverExpires Select-Object name Search-ADAccount -PasswordNeverExpires Set-ADUser -PasswordNeverExpires \$false Search-ADAccount -PasswordExpired Disable-ADAccount |
| Password expired accounts | Search-ADAccount -PasswordExpired -usersonly fl name |
| Password never expires accounts | Search-ADAccount -PasswordNeverExpires -usersonly fl name |
| Get Accounts inactive since date or days | Search-ADAccount -AccountInactive -DateTime " June 16" Search-ADAccount -AccountInactive -TimeSpan 1.12:00:00 # -TimeSpan Day.hour:minute:second |
| Account inactive for 30 days or more | Search-ADAccount -AccountInactive -TimeSpan 30.00:00:00 fl name |
| Move AD User to Organisation Unit | Get-ADUser test Move-ADObject -TargetPath "OU=Domain Users,DC=avtech,DC=loc" |

Backup Types

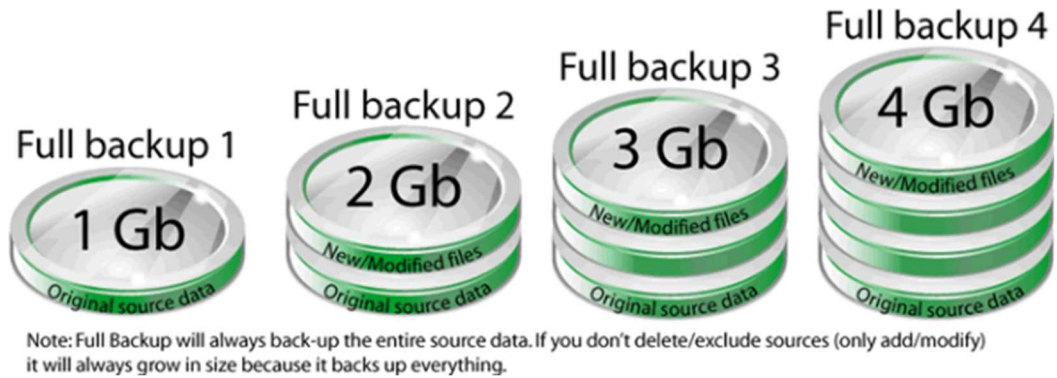
The image below provides an overview comparison between these backup types, for detailed information about each read the rest of the article:

| Backup type | Data backed up | Backup time | Restore time | Storage space |
|---------------------|---------------------------------|-------------|--------------|---------------|
| Full backup | All data | Slowest | Fast | High |
| Incremental backup* | Only new/modified files/folders | Fast | Moderate | Lowest |
| Differential backup | All data since last full | Moderate | Fast | Moderate |
| Mirror backup | Only new/modified files/folders | Fastest | Fastest | Highest |

○ *recommended backup type

Full backup

Full backup is the starting point for all other types of backup and contains all the data in the folders and files that are selected to be backed up. Because full backup stores all files and folders, frequent full backups result in faster and simpler restore operations. Remember that when you choose other **backup types**, restore jobs may take longer. As an example, for a full backup job that runs four times the representation below is conclusive on how the backed up data will grow with every run:



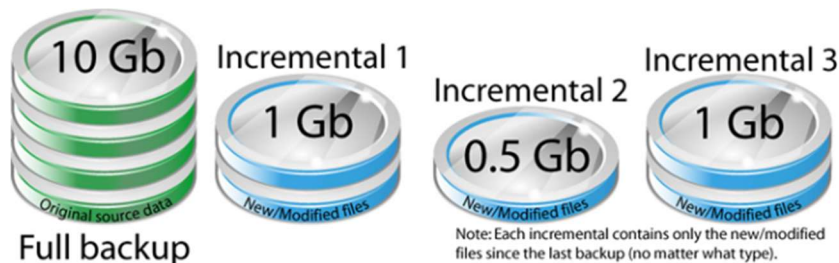
Differential backup

Differential backup contains all files that have changed since the last FULL backup. The advantage of a differential backup is that it shortens restore time compared to a full backup or an incremental backup. However, if you perform the differential backup too many times, the size of the differential backup might grow to be larger than the baseline full backup. In the image below you can see an example on how a differential backup would look like for a backup job that runs four times:



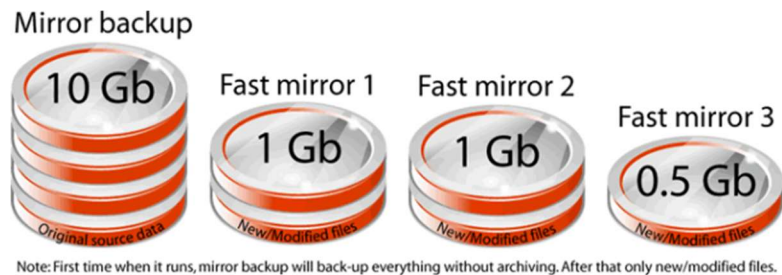
Incremental backup

Incremental backup stores all files that have changed since the last FULL, DIFFERENTIAL OR INCREMENTAL backup. The advantage of an incremental backup is that it takes the least time to complete. However, during a restore operation, each incremental backup must be processed, which could result in a lengthy restore job. The representation below shows how a backup job running four times would look like when using incremental.



Mirror backup

Mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the source data. It has the benefit that the backup files can also be readily accessed using tools like Windows Explorer.



How to Backup Active Directory Domain Services Database in Windows Server 2012 R2

Maintaining an AD DS Database is an important administrative task that you must schedule regular to ensure that, in the case of disaster. You can recover lost or corrupted data and repair the AD DS Database.

The AD DS has its own database engine, the Extensible Storage Engine (ESE), which manages the storage of all AD DS objects in an AD DS database. The AD DS database is stored as a file name Ntds.dit. When you install and configure AD DS, you can specify the location of the file. The default location is %SystemRoot%\NTDS.

AD DS includes the following files as in figure.

AD DS Database and Log Files

| File | Description |
|--|---|
| Ntds.dit | <ul style="list-style-type: none">• Main AD DS database file• Stores all AD DS objects on the domain controller• Use the default location <code>systemroot\NTDS</code> folder |
| Edb*.log | <ul style="list-style-type: none">• Is a transaction log file• Uses the default transaction log file <code>Edb.log</code> |
| Edb.chk | <ul style="list-style-type: none">• Is a Database checkpoint file• Tracks data not yet written to AD DS database file |
| Edbres00001.jrs Edbres00002.jrs | <ul style="list-style-type: none">• Are the reserved transaction log files that allows the directory to process transactions if the server runs out of disk space |

You can back up AD DS by using Windows Server Backup, Wbadmin.exe or PowerShell. Depending on the roles installed on the computer running Windows Server 2012 R2, the System State Data on a Domain Controller includes the following components:

- Active Directory Database (Ntds.dit)
- The SYSVOL shared folder
- The registry
- System startup files
- The COM+ Class Registration database
- Active Directory Certificate Services (AD CS) database
- Cluster service information
- Microsoft Internet Information Services (IIS) metadirectory
- System files under Windows Resource Protection

Backing up the System State in Windows Server 2012 R2 creates a point-in-time snapshot that you can use to restore a server to a previous working state. It does this using the Volume Shadow Copy Service (VSS). VSS helps to prevent inadvertent data loss.

To back up the System State Backup using the Graphical User Interface (GUI), perform the following steps:

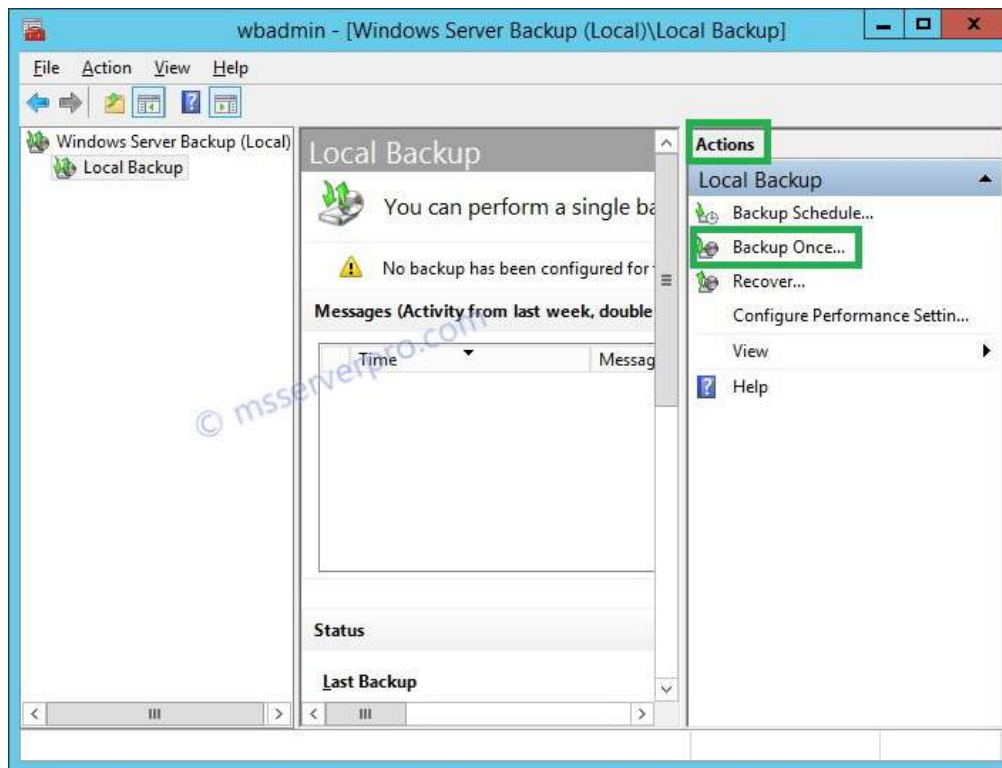
1. Log on to the domain controller with an account that is a member of the **Domain Admins** group and Open **Server Manager** from the **Taskbar**.



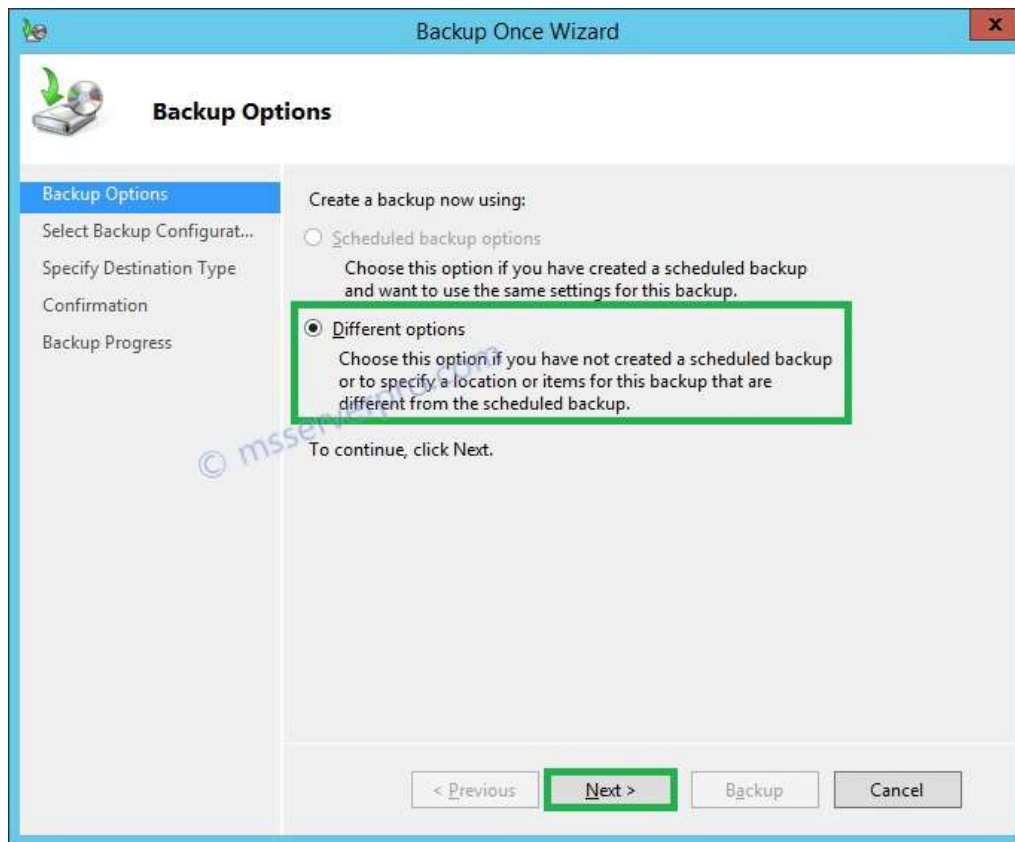
2. In the **Server Manager**, click the **Tools** Menu and select **Windows Server Backup**.



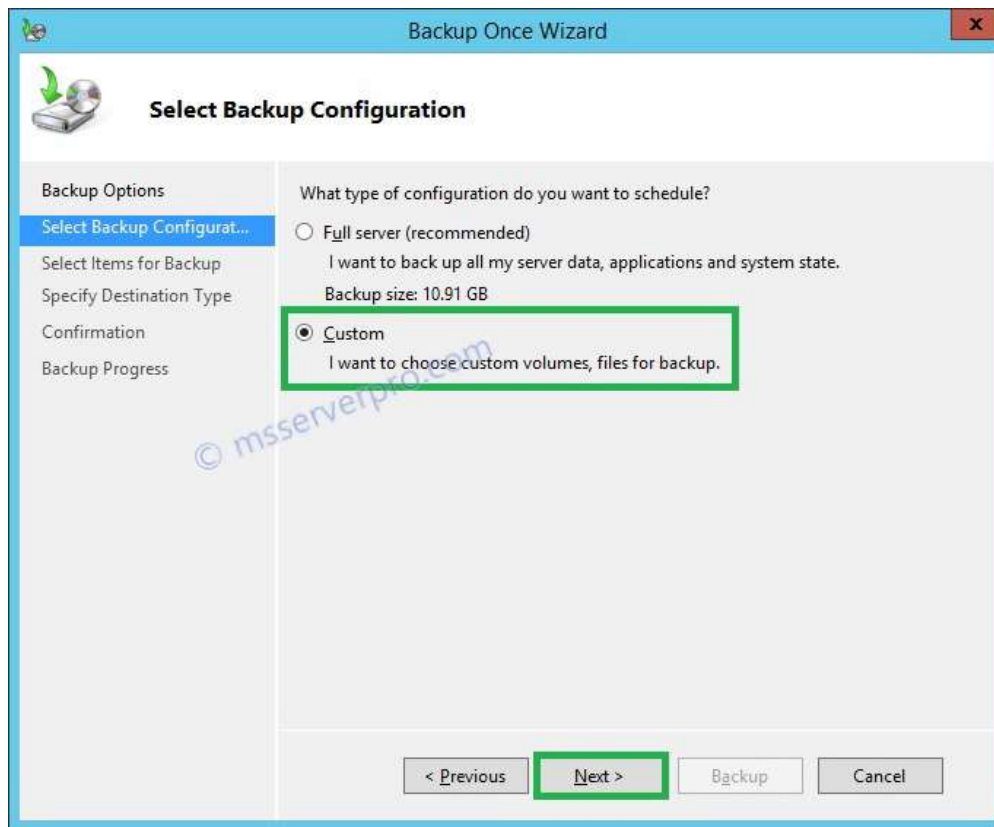
3. In the **Wbadmin (Windows Server Backup) Local** console, Click **Backup Once** in the **Actions** pane.



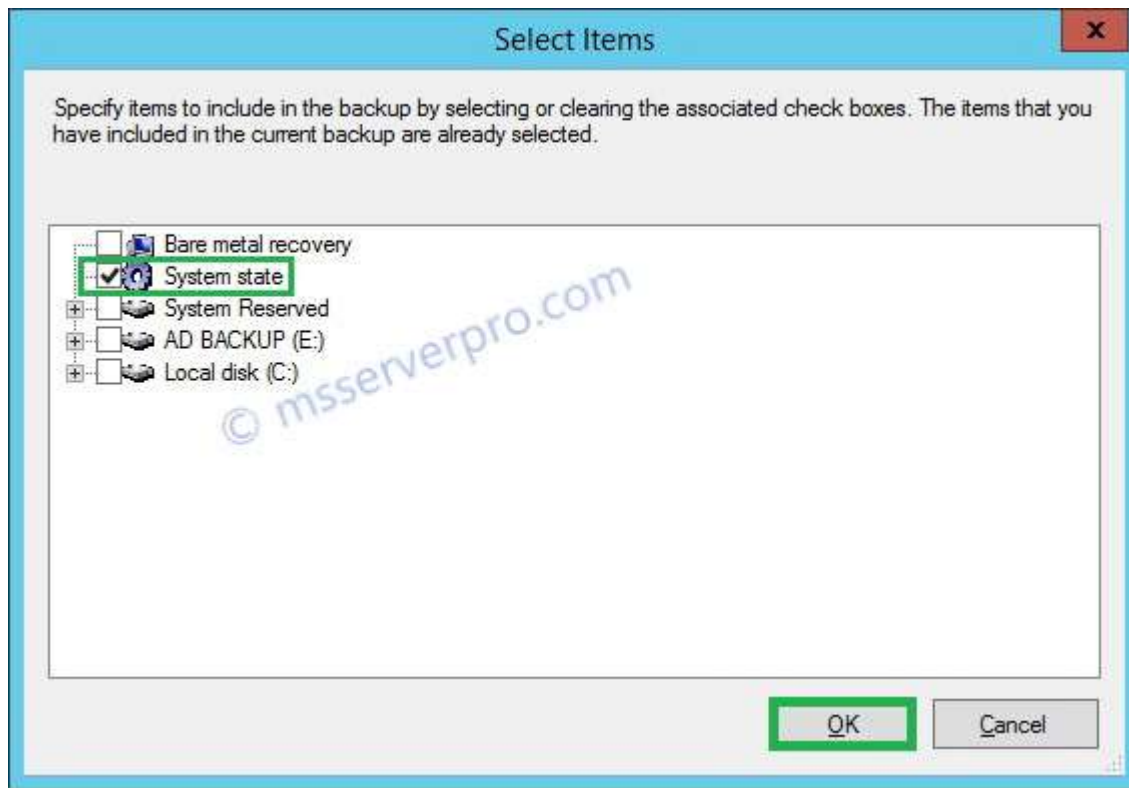
4. On the **Backup Once Wizard** page, click the **Different Options**, and then click **Next**.



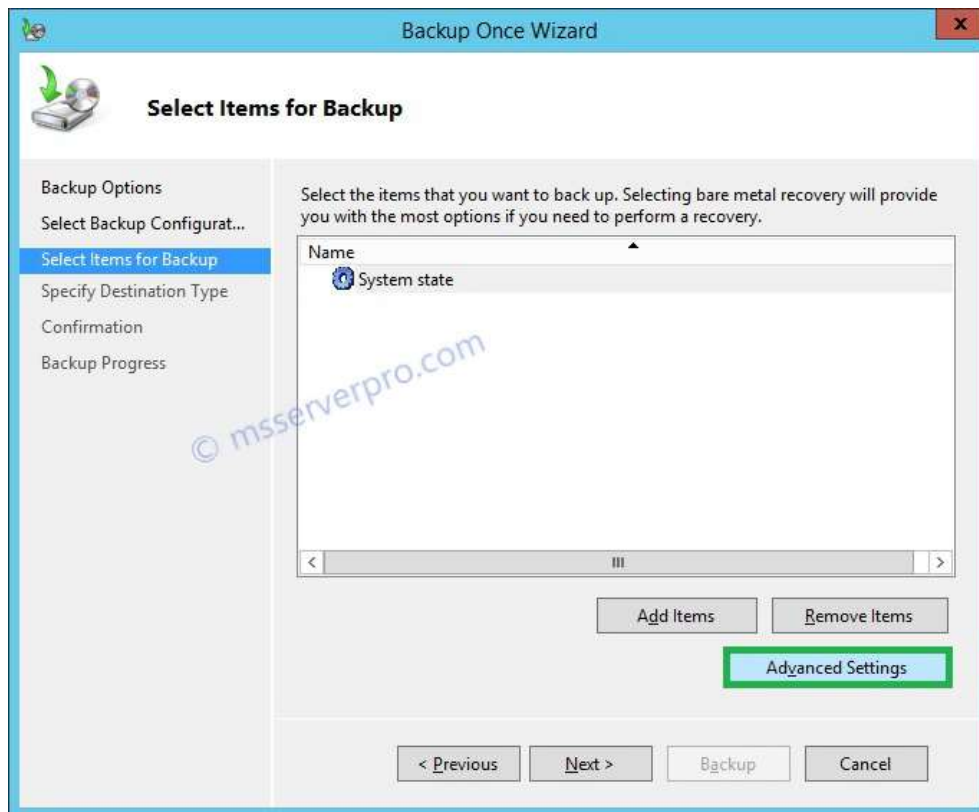
5. On the **Select Backup Configuration** page, click the **Custom** button, and then click **Next**.

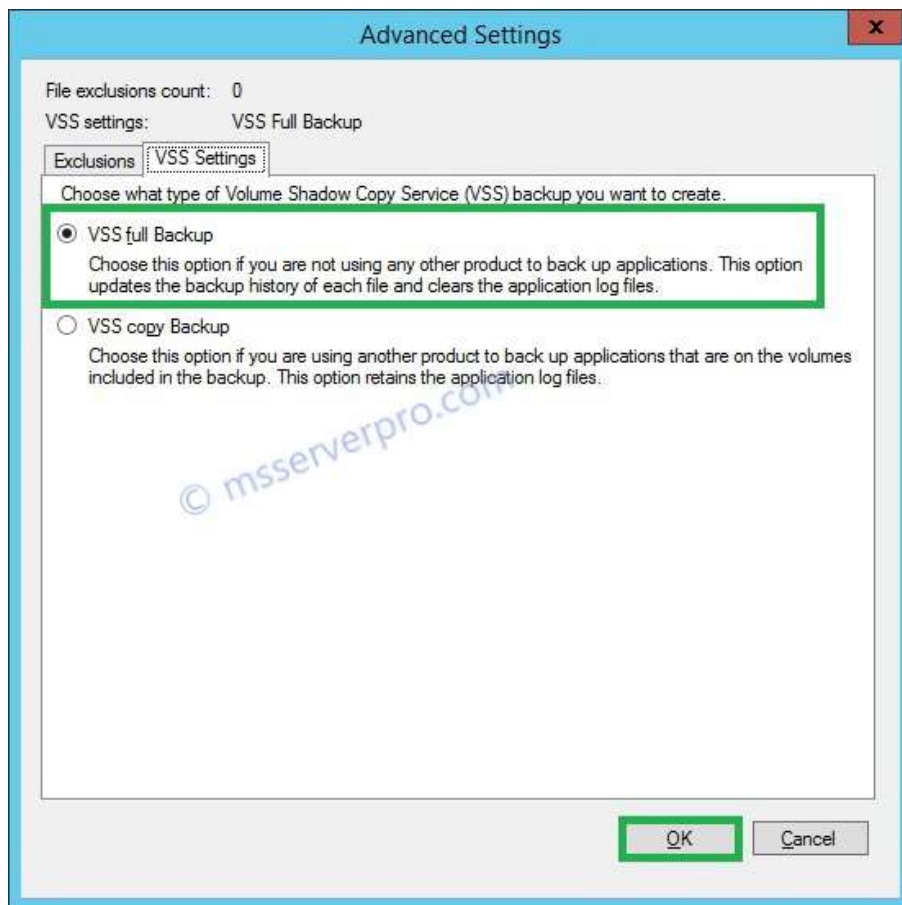


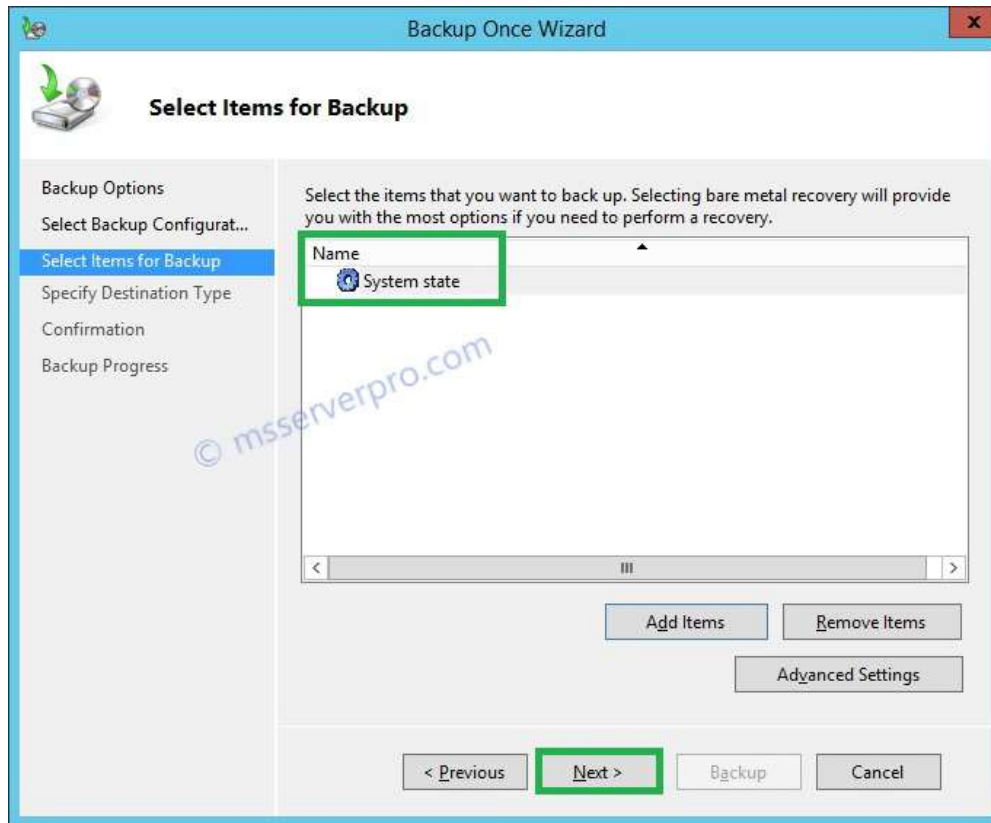
6. On the **Select Items for Backup** page, click the **Add Items** button. In the **Select Items** Windows, check **System state** check box, and then click **OK**.



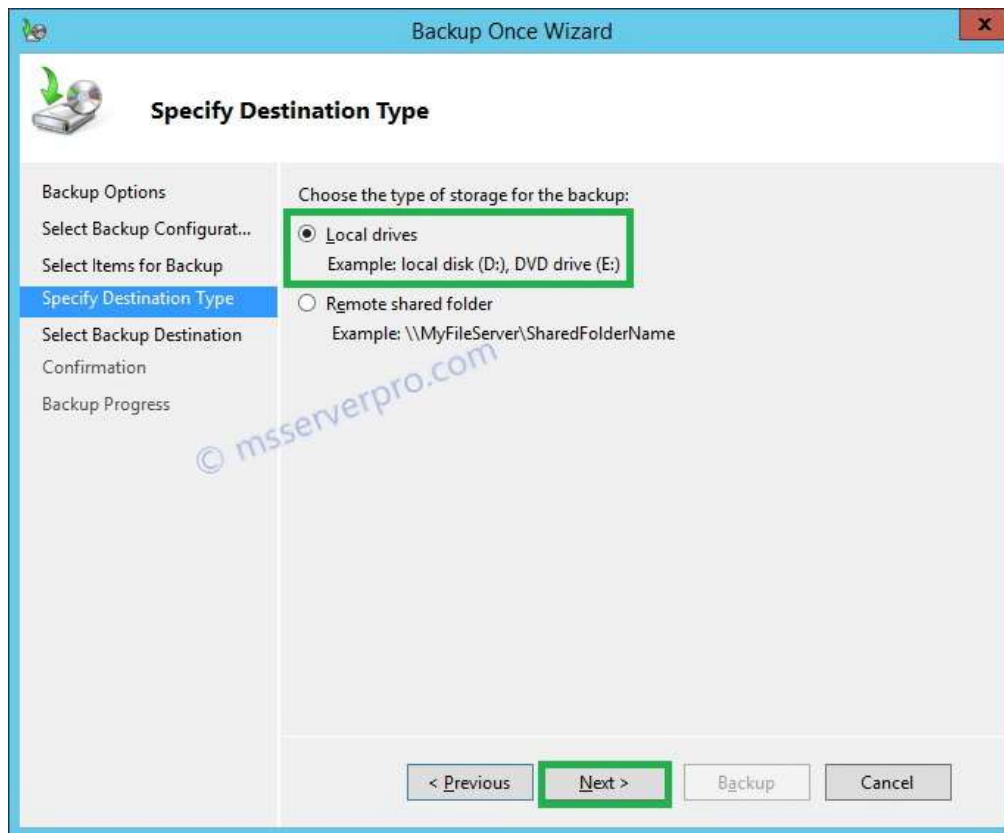
7. Back on the **Select Items for Backup** page, click **Advanced Settings**, and then click **VSS Settings** and select **VSS full backup** click **Next**.



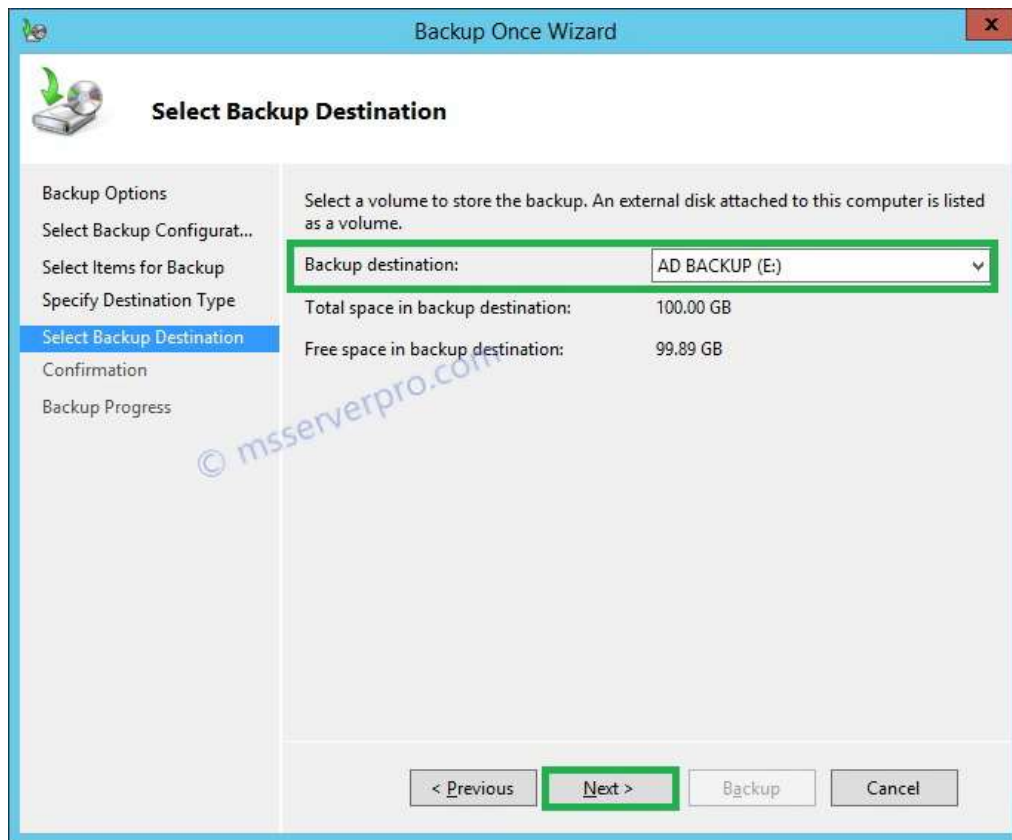




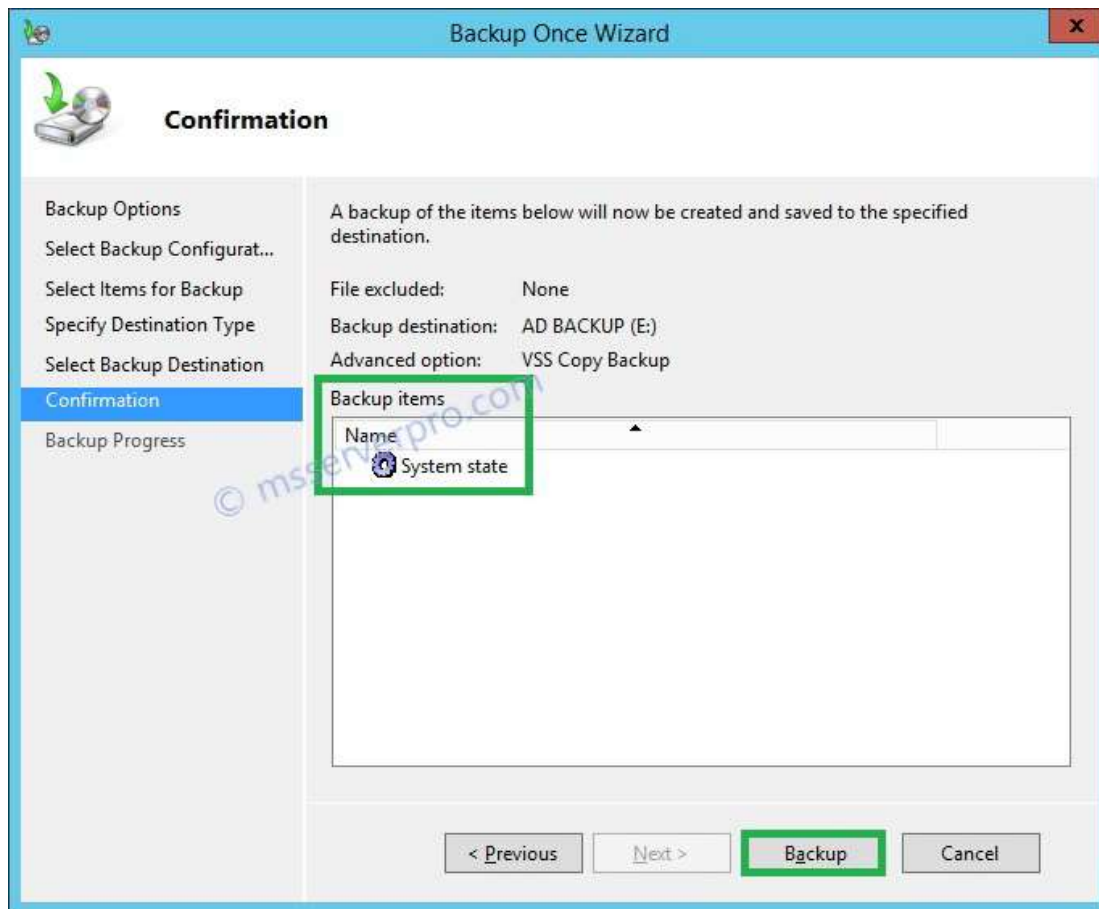
8. On the **Specify Destination Type** page, select either the **Local drives** or **Remote shared folder** button and click **Next**.



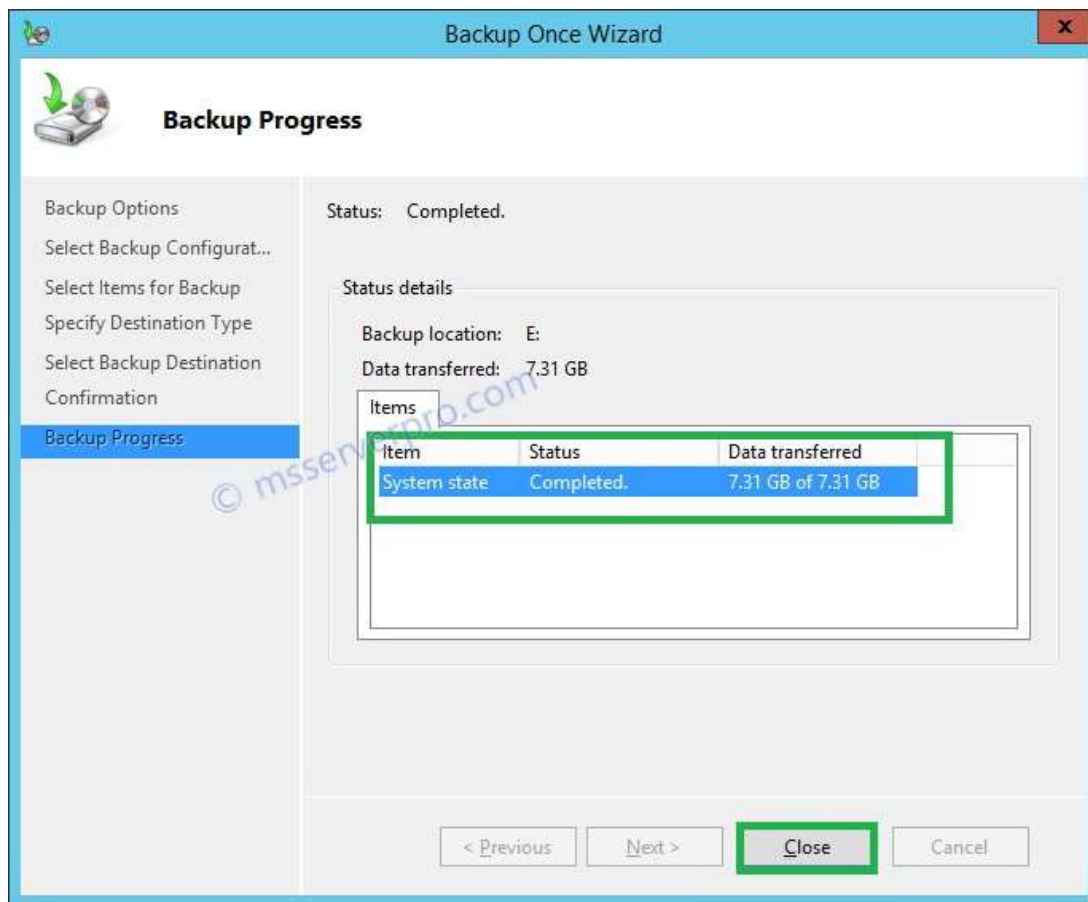
9. On the **Select Backup Destination** page, select the **backup destination** and then click **Next**.



10. On the **Confirmation** page review the **Backup items**, and then click **Backup** to continue..



11. On the **Backup Progress** page, **System state** backup status is **completed** and then clicks **Close**.



To back up System State through the Wbadmin.exe:

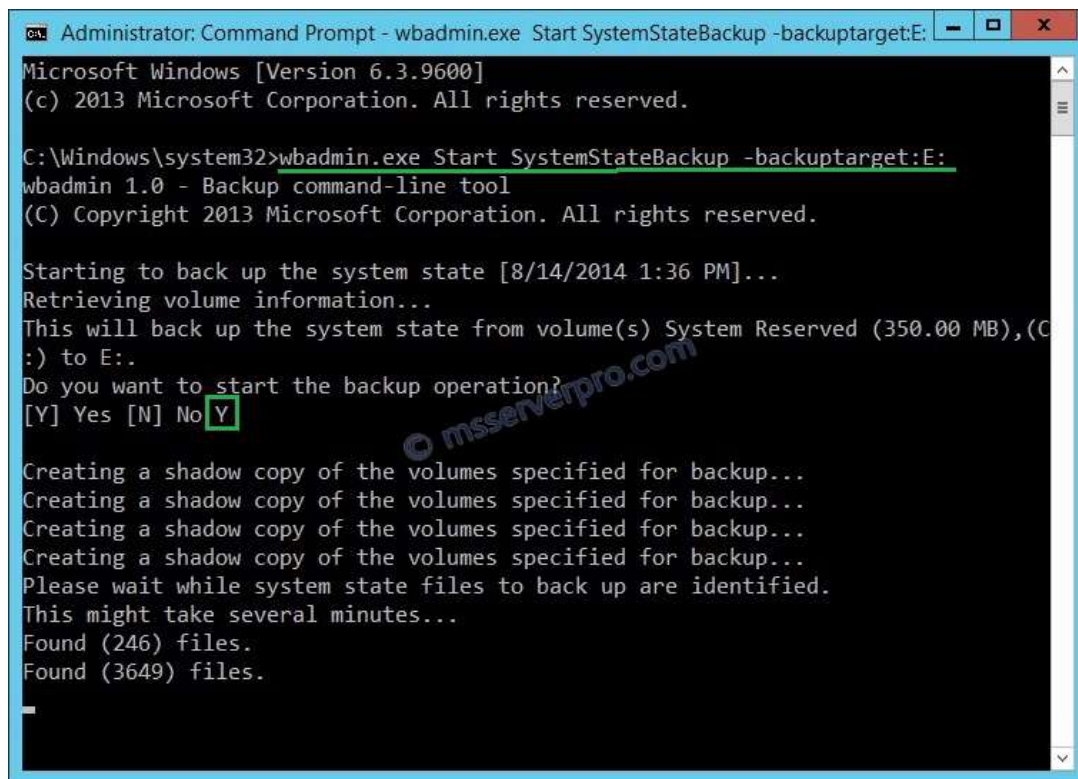
1. Open **Command Prompt (Admin)**.
2. In the Administrator: Command Prompt, type **wbadmin.exe Start SystemStateBackup**

-backuptarget:E:

This will back up the System State from volume(s) from Local Disk (C:) to E:.

Do you want to start the backup operation?

Type **Y** for Yes and Press **Enter**.



```
Administrator: Command Prompt - wbadmin.exe Start SystemStateBackup -backuptarget:E:
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

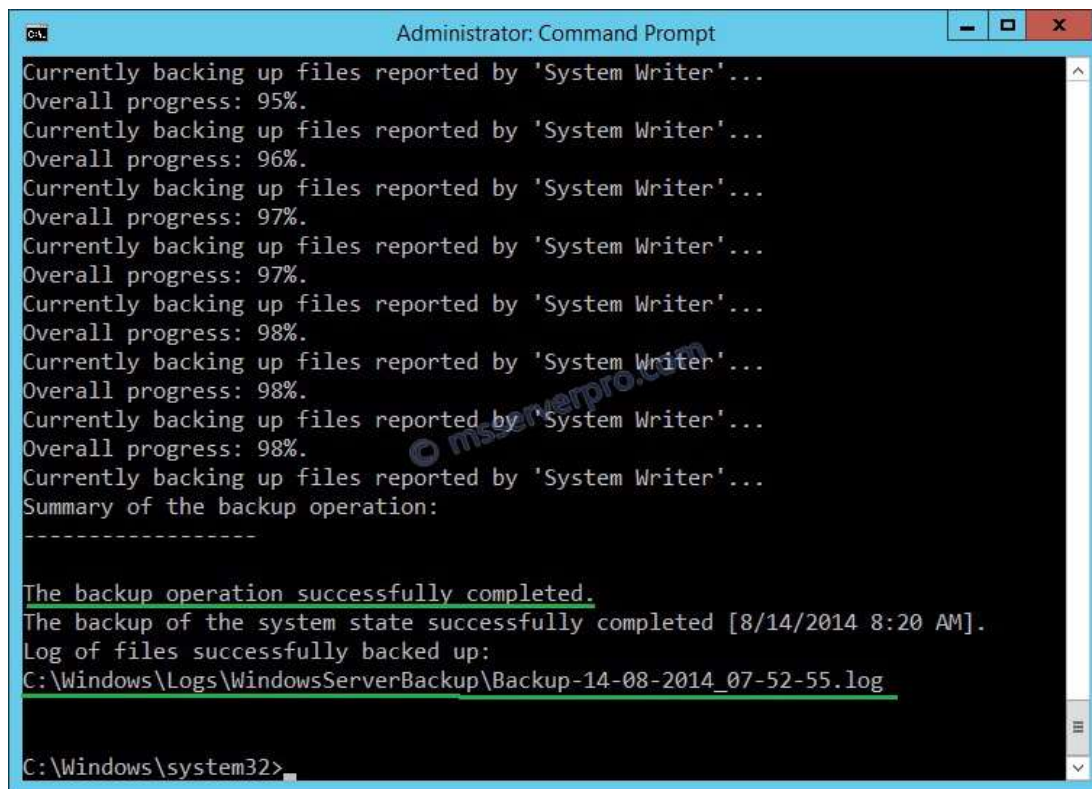
C:\Windows\system32>wbadmin.exe Start SystemStateBackup -backuptarget:E:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2013 Microsoft Corporation. All rights reserved.

Starting to back up the system state [8/14/2014 1:36 PM]...
Retrieving volume information...
This will back up the system state from volume(s) System Reserved (350.00 MB),(C:) to E:.
Do you want to start the backup operation?
[Y] Yes [N] No Y

Creating a shadow copy of the volumes specified for backup...
Creating a shadow copy of the volumes specified for backup...
Creating a shadow copy of the volumes specified for backup...
Creating a shadow copy of the volumes specified for backup...
Please wait while system state files to back up are identified.
This might take several minutes...
Found (246) files.
Found (3649) files.
```

Next, **Wbadmin.exe** creates the shadow copy of the C drive. After it does this it identifies the system state files to back up. Once it has completed its search for system state files, it begins the back up.

Figure shows that back up of system state completed successfully.



```
Administrator: Command Prompt
Currently backing up files reported by 'System Writer'...
Overall progress: 95%.
Currently backing up files reported by 'System Writer'...
Overall progress: 96%.
Currently backing up files reported by 'System Writer'...
Overall progress: 97%.
Currently backing up files reported by 'System Writer'...
Overall progress: 97%.
Currently backing up files reported by 'System Writer'...
Overall progress: 98%.
Currently backing up files reported by 'System Writer'...
Overall progress: 98%.
Currently backing up files reported by 'System Writer'...
Overall progress: 98%.
Currently backing up files reported by 'System Writer'...
Summary of the backup operation:
-----
The backup operation successfully completed.
The backup of the system state successfully completed [8/14/2014 8:20 AM].
Log of files successfully backed up:
C:\Windows\Logs\WindowsServerBackup\Backup-14-08-2014_07-52-55.log

C:\Windows\system32>
```

Once the backup is complete, **wbadmin.exe** creates a log with a naming convention of **System State Backup-14-08-2014_07-52-55.log**.

Backup-14-08-2014_07-52-55.log - Notepad

```
File Edit Format View Help
Backed up C:\Windows\WinSxS\x86_windowssearchengine-structuredquery_31bf3856ad364e35_7.0.91
Backed up C:\Windows\WinSxS\x86_windowssearchengine-structuredquery_31bf3856ad364e35_7.0.91
Backed up C:\Windows\WinSxS\x86_windowssearchengine-structuredquery_31bf3856ad364e35_7.0.91
Backed up C:\Windows\WinSxS\x86_wpf-presentationhostexe_31bf3856ad364e35_6.3.9600.16384_noi
Backed up C:\Windows\WinSxS\x86_wpf-presentationhostproxy_31bf3856ad364e35_6.3.9600.16384_
Backed up C:\Windows\WinSxS\x86_wsapi.resources_31bf3856ad364e35_6.3.9600.16384_en-us_afd
Backed up C:\
Backed up C:\Windows\
Backed up C:\Windows\System32\
Backed up C:\Windows\System32\wbem\
Backed up C:\Windows\System32\wbem\Repository\
Backed up C:\Windows\System32\wbem\Repository\INDEX.BTR
Backed up C:\Windows\System32\wbem\Repository\MAPPING1.MAP
Backed up C:\Windows\System32\wbem\Repository\MAPPING2.MAP
Backed up C:\Windows\System32\wbem\Repository\MAPPING3.MAP
Backed up C:\Windows\System32\wbem\Repository\OBJECTS.DATA
Backed up C:\
Backed up C:\Windows\
Backed up C:\Windows\NTDS\
Backed up C:\Windows\NTDS\edb.log
Backed up C:\Windows\NTDS\edb00003.log
Backed up C:\Windows\NTDS\edb.chk
Backed up C:\Windows\NTDS\ntds.dit
```