

ABS Enterprise®

Pre-Installation Guide – SPX [Hyper-V]

April 2020



Contents

Preamble	3
Service Account Creation & Basic Permissions	4
Appliance: Network Configuration.....	6
Clients: System Check.....	8
Pre-install Checklist.....	13

Preamble

Operating Systems

- Windows 2019
- Windows 2016
- Windows 2012
- Windows 2008 R2
- Windows 2008 SP2
- Windows SBS 2011/2008
- Windows 10/8/7/Vista/XP SP3

File Systems

- FAT16, FAT16X
- FAT32, FAT32X
- NTFS
- MBR Disks
- ReFS
- GPT Disks
- Basic and Dynamic Volumes and Disks
- 4K/AF drives with 4096-byte physical sectors and 512-byte sector emulation

Notes

- 1 Gb network strongly recommended
- A reboot is required after agent installation

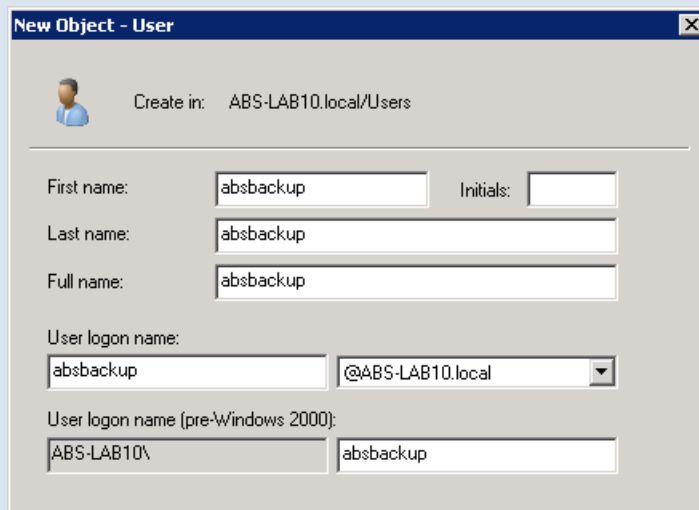
Not Supported

- Windows Storage Spaces storage pools
- Windows Server Cluster Shared Volumes

Service Account Creation & Basic Permissions

1. Create the User in Active Directory

- In Active Directory Users & Computers (AD), create a new user with a logon name of **absbackup**
- Make sure that **User cannot change password** and **Password never expires** are selected



New Object - User

Create in: ABS-LAB10.local/Users

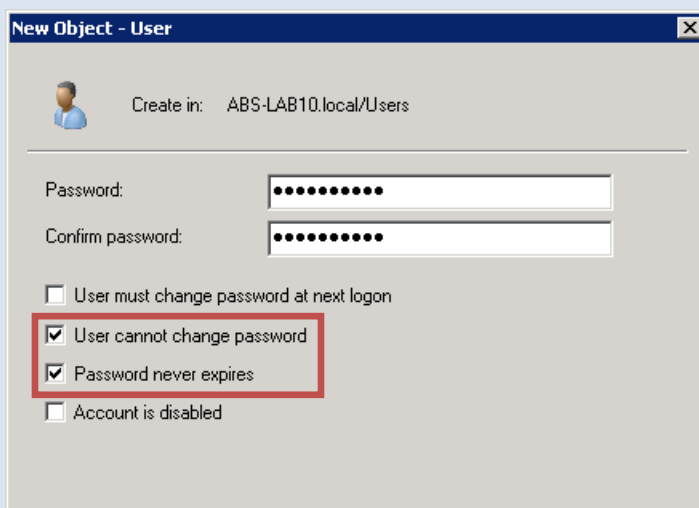
First name: absbackup Initials:

Last name: absbackup

Full name: absbackup

User logon name: absbackup @ABS-LAB10.local

User logon name (pre-Windows 2000): ABS-LAB10\ absbackup



New Object - User

Create in: ABS-LAB10.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

2. Adjust Account Permissions

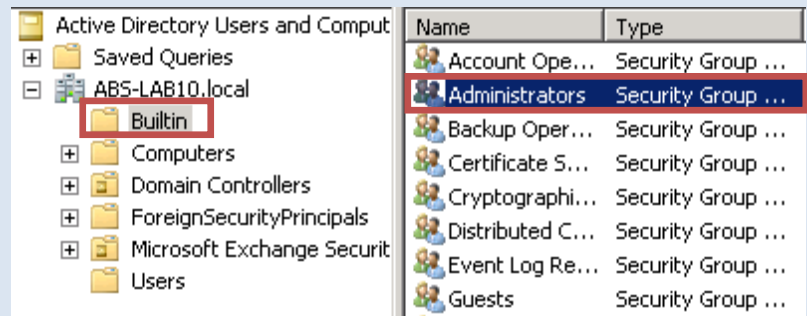
- In **AD** click on the Users OU. Then on the right side pane, double click the **"Domain Admins"** Security Group - add the **absbackup** user to this group

Active Directory Users and Comput		Name	Type
<div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> </div>	Saved Queries	Allowed RODC Password ...	Security Group ...
	ABS-LAB10.local	Cert Publishers	Security Group ...
	Builtin	Denied RODC Password ...	Security Group ...
	Computers	DiscoverySearchMailbox ...	User
	Domain Controllers	DnsAdmins	Security Group ...
	ForeignSecurityPrincipals	DnsUpdateProxy	Security Group ...
	Microsoft Exchange Securit	Domain Admins	Security Group ...
	Users	Domain Computers	Security Group ...

3. Builtin Administrators

! When backing up domain controllers, add the **absbackup** user account to the **builtin administrators** group

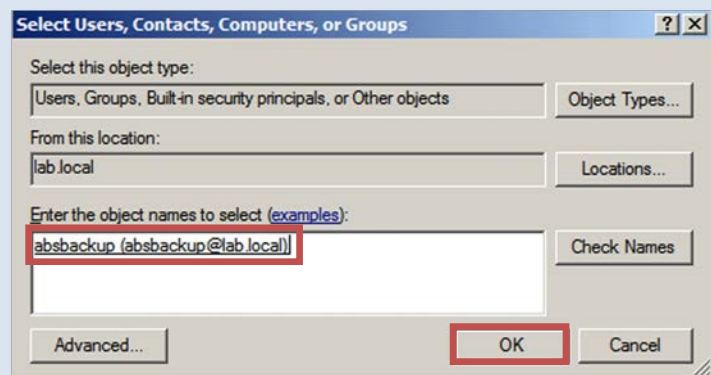
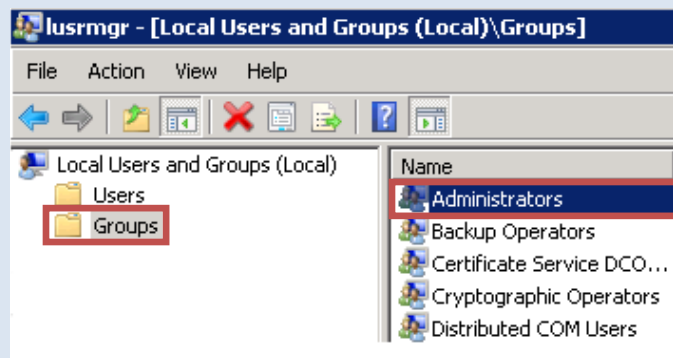
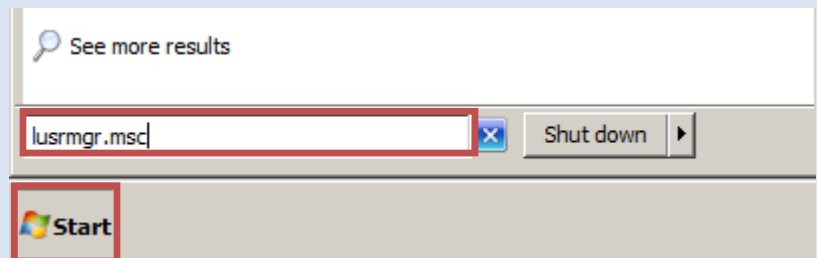
- In AD, click on the **Builtin OU**, double click the **Administrators** group - add the **absbackup** user



4. Local Administrator

- Click the **Start Button**
- Type in **lusrmgr.msc**, hit **Enter**
- Click on groups - add the **absbackup** user to the **Administrators** group

! Repeat step 4 on **all machines** being added for protection



Appliance: Network Configuration

1. Confirm Network Settings for the ABS Appliance®

If there is a content filter/proxy on the network, the appliance must be exempt from the content/filter proxy

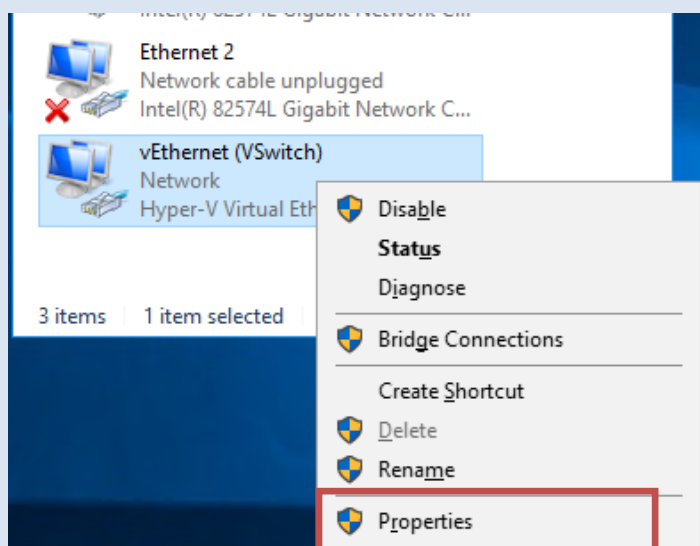
TCP Ports 20, 21, 25, 443, 1100-1200, 5556 and 8443 need to be allowed outbound from the appliance. *(443, 5556 and 8443 should be allowed for the client/protected machines.)*

The following ports may need to be allowed as noted:

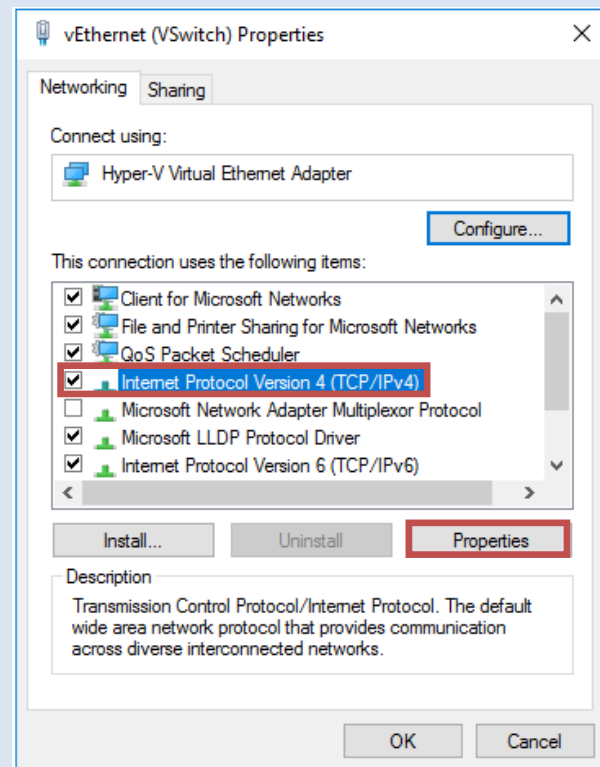
TCP 139, 445 + UDP 137, 138 (SMB/CIFS)
TCP 443, 902 (Ports required for appliance to restore directly to VMware datastore)
TCP 13581 (SPX console connection from ABS device to protected machines)

2. Assign a static IP to the Appliance

- Connect a keyboard, monitor, and mouse to the appliance
- Using Control Panel, Settings or via Windows Explorer; go to Network Properties or Network Connections and then Adapter Settings
- Right-click on **VSwitch**, select **Properties**



- d. Highlight **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**



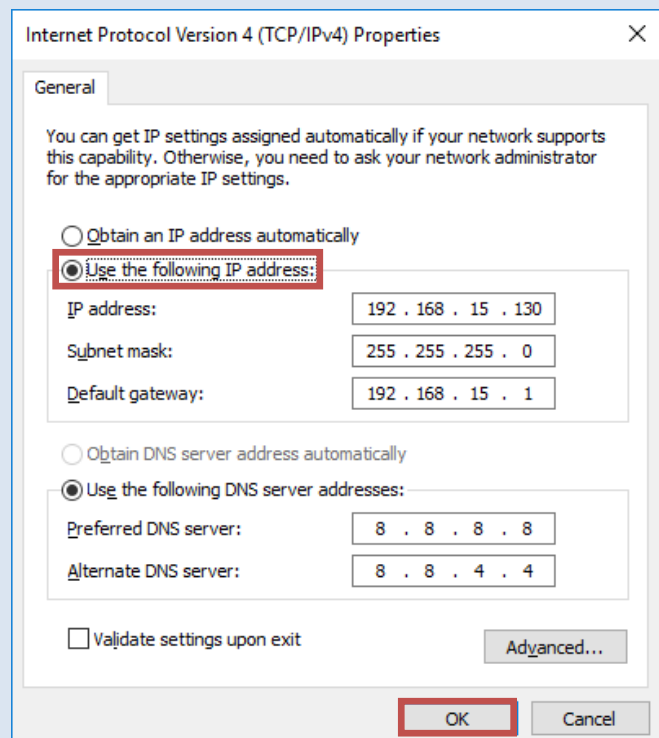
- e. Select **Use the following IP address**, fill in the required information


- f. Under DNS:

Use your company's DNS for the Preferred DNS Server

Use the following for the Alternate DNS Server: 8.8.8.8

Click **OK**




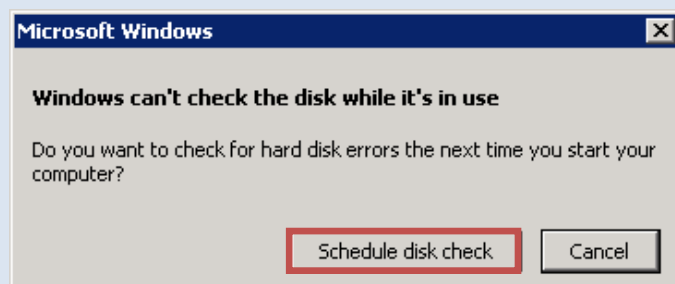
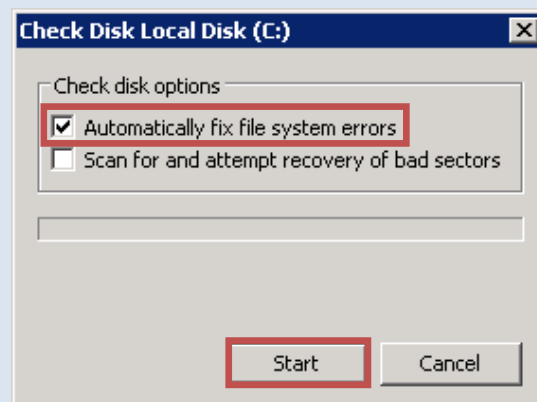
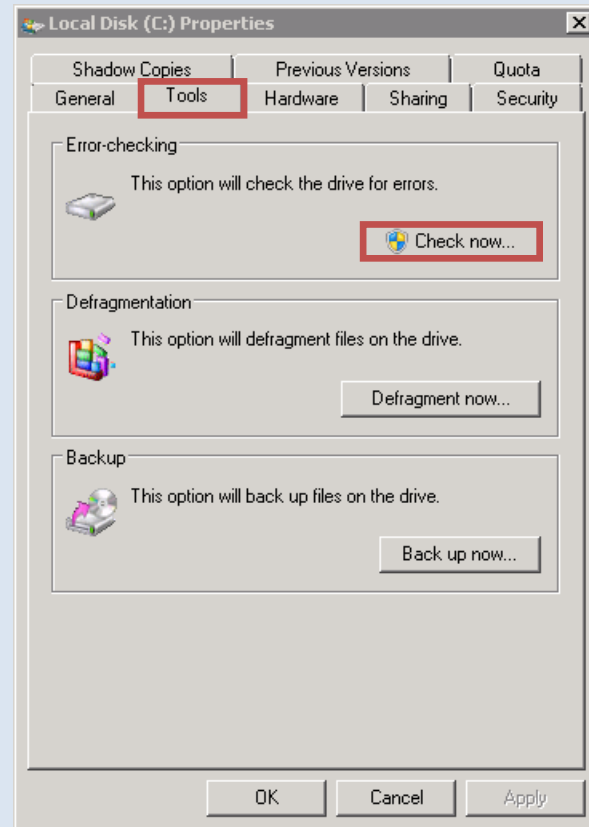
 Please **Reboot** the appliance.
(ImageManager will not work until the appliance is rebooted.)

Clients: System Check

1. Error Checking on Client (Protected) Machines

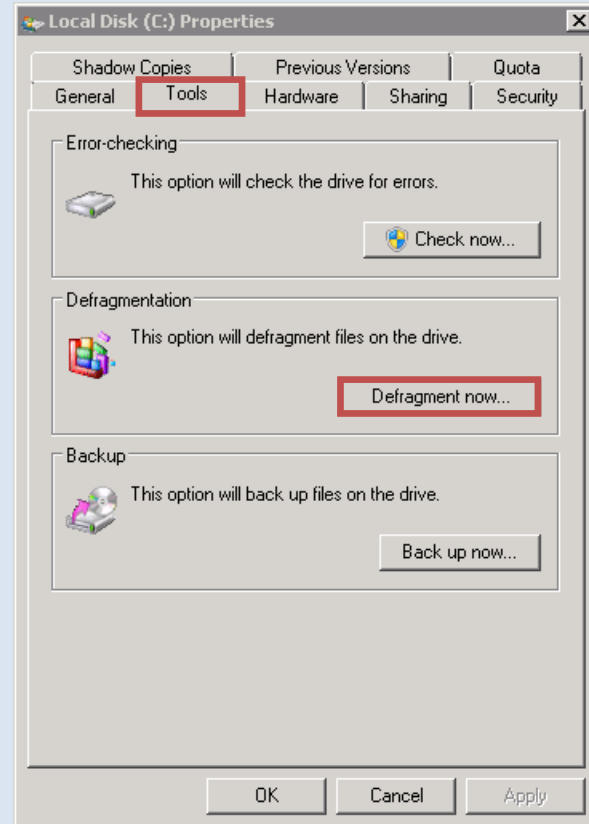
- Go to the **Local Disk Properties**
- From the **Tools** tab, click **Check Now**
- Make sure "Automatically fix file system errors" is checked, click **Start**
- Click on **Schedule disk check**
- Reboot** machine when convenient

 This process should not be interrupted. Give ample time on next reboot.




2. Disk Defrag

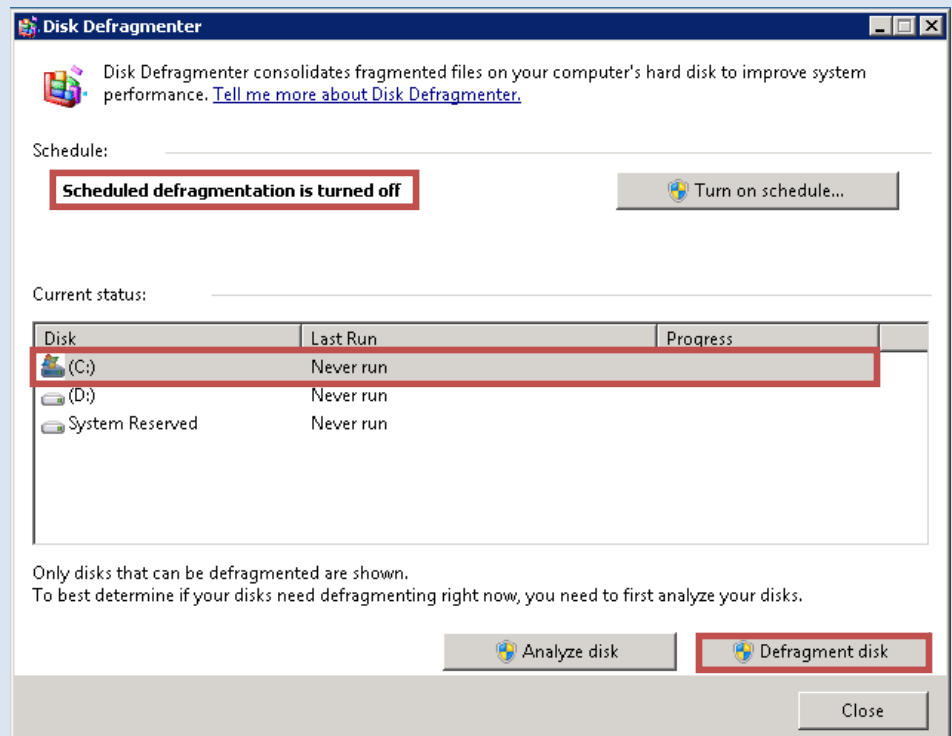
- a. From the **Tools** tab, click on **Defragment Now**



- b. Select a volume (or all volumes if possible) and click **Defragment/Optimize Now**

 Repeat this step for all volumes being added for protection if done individually.

- c. Make sure that disk defrag is **not** set to run on a schedule



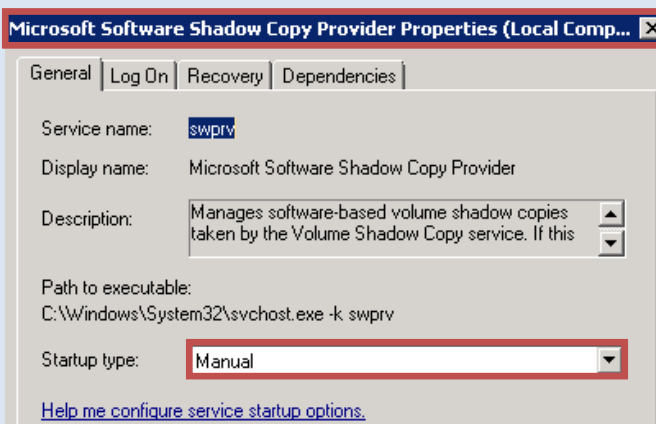
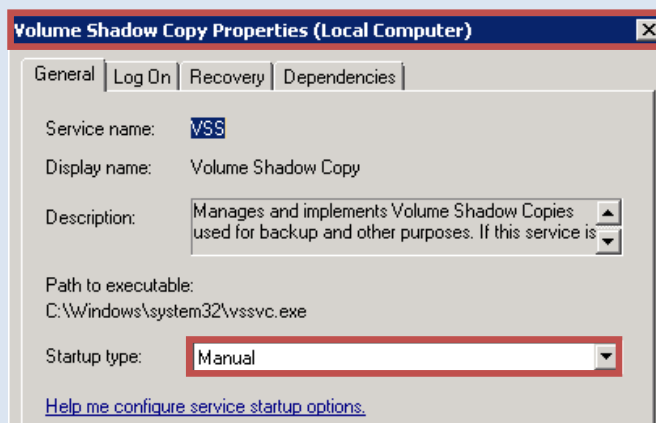
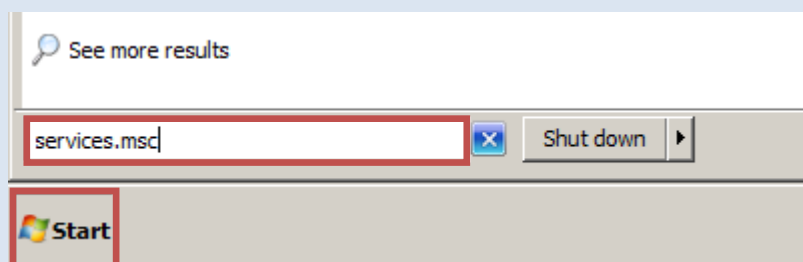
3. Services

Make sure the following services are set to a **Manual** startup type:

- **Volume Shadow Copy** service
- **Microsoft Software Shadow Copy Provider** service

To Check:

- a. Click **Start**
- b. Type in **services.msc**, hit **Enter**
- c. Double click each service
- d. Make sure startup type is set to **Manual**




4. VSS Writers

Check the status of the VSS writers – ensure they are in a stable state

To Check:

- Click Start
- Type in **CMD**, hit **Enter**
- Type in:
vssadmin list writers, hit **Enter**
- The state for each writer should be listed as **Stable**


 If you have an issue running the commands, you may need to run the command prompt with elevated rights. In that case, right click on the CMD prompt icon, and select **"Run as Administrator"**

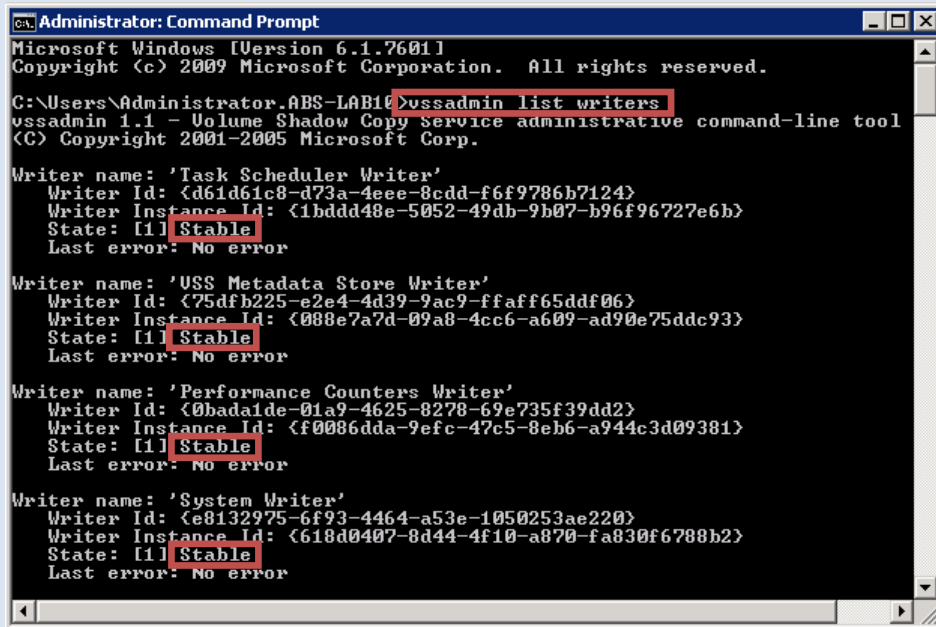
5. VSS Providers

Check and make sure there is only one VSS provider (and that it is issued by Microsoft)

To Check:

- In command prompt, type in:
vssadmin list providers

 If there is more than one listed, it should be removed - this avoids VSS provider conflict when protecting.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

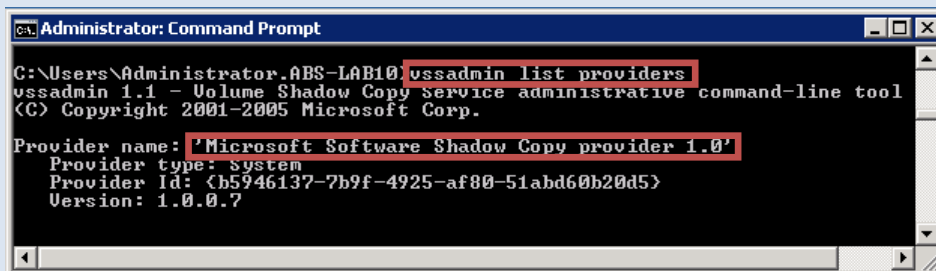
C:\Users\Administrator.ABS-LAB10>vssadmin list writers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Writer name: 'Task Scheduler Writer'
Writer Id: {d61d61c8-d73a-4eee-8cdd-f6f9786b7124}
Writer Instance Id: {1bddd48e-5052-49db-9b07-b96f96727e6b}
State: [1] Stable
Last error: No error

Writer name: 'VSS Metadata Store Writer'
Writer Id: {75dfb225-e2e4-4d39-9ac9-ffaff65ddf06}
Writer Instance Id: {008e7a7d-09a8-4cc6-a609-ad90e75ddc93}
State: [1] Stable
Last error: No error

Writer name: 'Performance Counters Writer'
Writer Id: {0bada1de-01a9-4625-8278-69e735f39dd2}
Writer Instance Id: {f0086dda-9efc-47c5-8eb6-a944c3d09381}
State: [1] Stable
Last error: No error

Writer name: 'System Writer'
Writer Id: {e8132975-6f93-4464-a53e-1050253ae220}
Writer Instance Id: {618d0407-8d44-4f10-a870-fa830f6788b2}
State: [1] Stable
Last error: No error
```



```
Administrator: Command Prompt

C:\Users\Administrator.ABS-LAB10>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Provider name: 'Microsoft Software Shadow Copy provider 1.0'
Provider type: system
Provider Id: {b5946137-7b9f-4925-af80-51abd60b20d5}
Version: 1.0.0.7
```

6. Uninstall Software

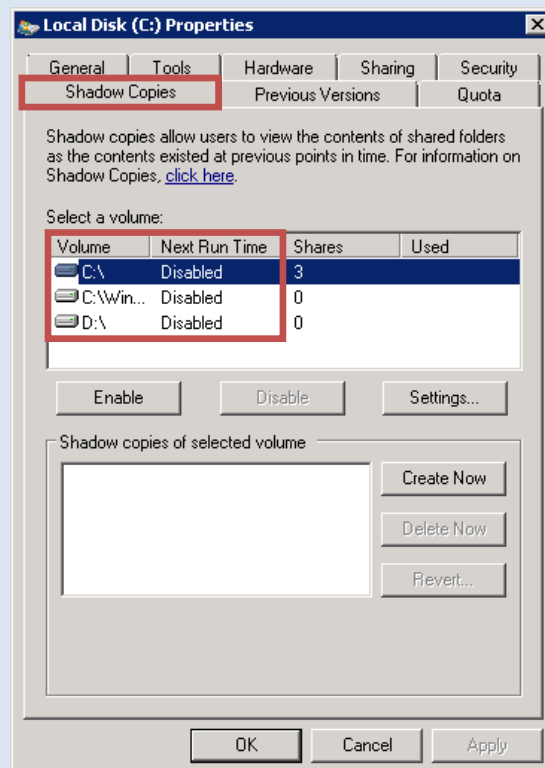
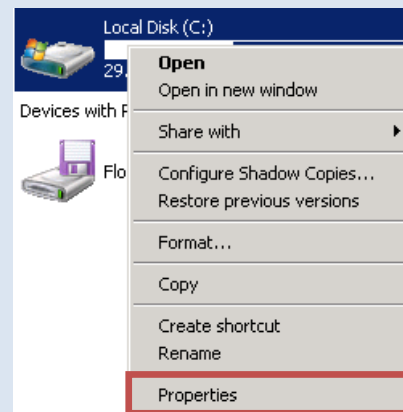
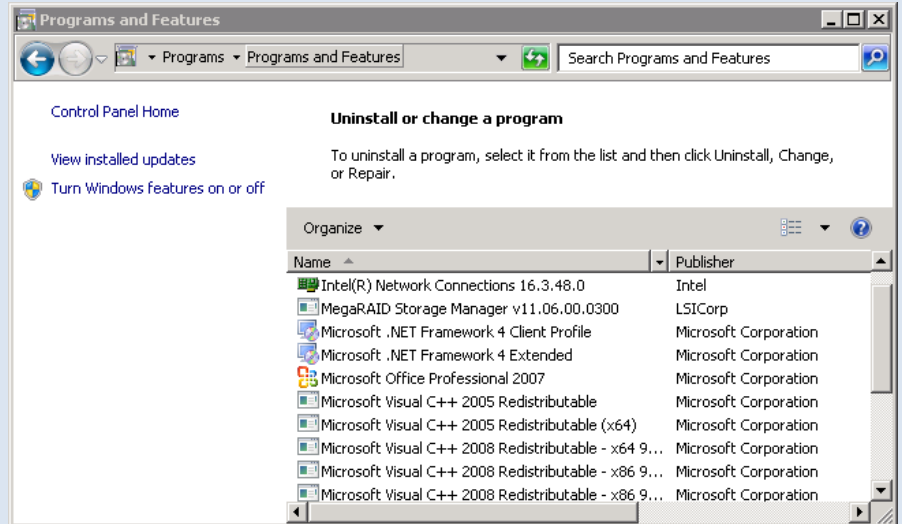
Ensure that other image based backup software is uninstalled (i.e. Acronis)

! Having multiple image based backup software installed could cause the server to bluescreen during a backup job

7. Disable Microsoft Volume Snapshots

- Click **Start**
- Click **Computer**
- Right click a local disk, go to **Properties**
- Click the **Shadow Copies** tab. From there you can confirm/disable **Shadow Copies** for all the local disks on the server

! Repeat **Steps 1-7** on **all machines** being added for protection



Pre-install Checklist

This list below will help you keep track of the various tasks which need to be performed.

Steps	Done	Notes
Service Account Creation		
Added to Domain Admins group		
Added to BuiltIn Administrators group		
Appliance Network Configuration		
Set static IP on appliance		
Confirm network settings (ports 21, 25, 443, 1100-1200, 5556 and 8443 TCP outgoing are allowed & appliance is exempt from any filtering)		
These ports <i>may</i> need to be allowed as noted in specific cases TCP 139, 445 + UDP 137, 138 (SMB/CIFS) TCP 443, 902 (Ports required for ABS device to restore directly to VMware datastore) TCP 13581 (SPX console connection from ABS device to protected machines)		
Clients: System Check (for each client)		
Run error checking on all volumes		
Run defrag on all volumes		
Set Volume Shadow Copy & Microsoft Software Shadow Copy Provider services to manual		
Make sure VSS writers are stable (vssadmin list writers)		
Make sure there is only one VSS provider (vssadmin list providers)		
Make sure all other image based backup software is removed		
Disable MS Volume Snapshots on all volumes		
Add absbackup to local Administrator group (lusrmgr.msc)		
Reboot client machine(s) in order for scheduled disk checks to run		