1.a. You are the IT manager for a commercial company with headquarters in San Francisco and branches in Cleveland and Baton Rouge. How would you deploy SNMP...

The following is information on how to deploy SNMP using steps from Microsoft Support:

HOW TO: Configure the Simple Network Management Protocol (SNMP) Service in Windows Server 2003
For a Microsoft Windows 2000 version of this article, see 315154.

IN THIS TASK SUMMARY:
-How to Configure SNMP Agent Information
-How to Configure SNMP Communities and Traps
-How to Configure SNMP Security

Summary
This step-by-step article describes how to configure the Simple Network Management Protocol (SNMP) Service in Windows Server 2003. This article describes how to configure SNMP agent properties, SNMP traps, and SNMP security.

The SNMP Service, when configured for an agent, generates trap messages that are sent to a trap destination, if any specific events occur. For example, you can configure the SNMP service to send a trap when it receives a request for information that does not contain the correct community name and does not match an accepted host name for the service.

HOW TO: Configure SNMP Agent Information:

To configure SNMP agent information:
1. Click Start, point to Control Panel, point to Administrative Tools, and then click Computer Management.
2. In the console tree, expand Services and Applications, and then click Services.
3. In the right pane, double-click SNMP Service.
4. Click the Agent tab.
5. Type the name of the user or administrator of the computer in the Contact box, and then type the physical location of the computer or contact in the Location box.

These comments are treated as text and are optional.

6. Under Service, click to select the check boxes next to the services that are provided by your computer. Service options are:

Physical: Specifies whether the computer manages physical devices, such as a hard disk partition.
Applications: Specifies whether the computer uses any programs that send data by using TCP/IP.
Datalink and subnetwork: Specifies whether this computer manages a TCP/IP subnetwork or datalink, such as a bridge.
Internet: Specifies whether this computer acts as an IP gateway (router).
End-to-end: Specifies whether this computer acts as an IP host.

7. Click OK.

NOTE: If you have installed additional TCP/IP network devices, such as a switch or a router, see Request for Comments (RFC) 1213 for additional information. To view RFC 1213, visit the following Internet Engineering Task Force (IETF) Web site:
http://www.ietf.org/rfc/rfc1213.txt

Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

HOW TO: Configure SNMP Communities and Traps:

To configure traps:
1. Click Start, point to Control Panel, point to Administrative Tools, and then click Computer Management.
2. In the console tree, expand Services and Applications, and then click Services.
3. In the right pane, double-click SNMP Service.
4. Click the Traps tab.
5. In the Community name box, type the case-sensitive community name to which this computer will send trap messages, and then click Add to list.
6. Under Trap destinations, click Add.
7. In the Host name, IP or IPX address box, type the name, IP or IPX address of the host, and then click Add.

The host name or address appears in the Trap destinations list.

8. Repeat steps 5 through 7 to add the communities and trap destinations that you want.
9. Click OK.

HOW TO: Configure SNMP Security
To configure SNMP security for a community:
1. Click Start, point to Control Panel, point to Administrative Tools, and then click Computer Management.
2. In the console tree, expand Services and Applications, and then click Services.
3. In the right pane, double-click SNMP Service.
4. Click the Security tab.
5. Click to select the Send authentication trap check box (if it is not already selected) if you want a trap message sent whenever authentication fails.
6. Under Accepted community names, click Add.
7. To specify how the host processes SNMP requests from the selected community, click the permission level that you want in the Community Rights box.
8. In the Community Name box, type the case-sensitive community name that you want, and then click Add.
9. Specify whether or not to accept SNMP packets from a host. To do so, do one of the following:
-To accept SNMP requests from any host on the network, regardless of identity, click Accept SNMP packets from any host.
-To limit the acceptance of SNMP packets, click
Accept SNMP packets from these hosts, click Add, and then type the appropriate host name, IP or IPX address in the Host name, IP or IPX address box.
10. Click Add.
11. Click OK.

IMPORTANT: If you remove all of the community names, including the default name "Public", SNMP does not respond to any community names that are presented.

References
For additional information about how to configure network security for the SNMP service, click the following article number to view the article in the Microsoft Knowledge Base:
324261 Configure Network Security for the SNMP Service in Windows Server 2003

Last Updated: Jul 11, 2017

Microsoft Support
-https://support.microsoft.com/en-us/help/324263/how-to-configure-the-simple-network-management-protocol-snmp-service-i

Simple Network Management Protocol (SNMP) - A protocol used to monitor and manage network devices, such as routers, switches, and servers.

****

1.b.

...what are the advantages of using switches and routers with SNMP versus unmanaged appliances.

- The key difference between a managed and unmanaged switch is the ability to configure the switch and to prioritize LAN traffic to ensure that the most important information, as I have defined it, gets through.
- Managed switches give you more control over your LAN traffic and offer advanced features to control that traffic.
- An unmanaged switch simply allows Ethernet devices to communicate with one another, such as a PC or network printer, and those are typically what we call “plug and play.” They are shipped with a fixed configuration and do not allow any changes to this configuration.
- Unmanaged switch allows devices to talk to each other, but that is pretty much all that they do.
- Managed switches provide all the features of an unmanaged switch and provide the ability to configure, manage, and monitor your LAN. This gives you greater control over how data travels over the network and who has access to it.
- Also, managed switches use protocols such as the Simple Network Management Protocol, or what we call SNMP, for monitoring the devices on the network. SNMP is a protocol that facilitates the exchange of management information between network devices. SNMP queries can determine the health of the network or the status of a particular device. By displaying this data in an easily understood format, IT managers located at a central site can monitor the performance of the network and quickly detect and repair network problems without having to physically interact with the switch.
- SNMP allows me to remotely monitor my network devices, and I don’t have to go to the site to make changes or troubleshoot the switch.

Cisco Unmanaged versus Managed Switches
-https://www.cisco.com/c/dam/en/us/products/switches/networking_solutions_products_genericcontent0900aecd806c7afe.pdf

****

2.

Logon to any Windows 7, 8 or Windows Server and navigate your way to the Windows log section.

How many log files do you see? Which one(s) are the most important? And why?

Log files
Applies to: Windows 10

Log File	Phase: Location	Description	When To Use
setupact.log	Down-Level: $Windows.~BT\Sources\Panther	Contains information about setup actions during the downlevel phase.	All down-level failures and starting point for rollback investigations. This is the most important log for diagnosing setup issues.
	OOBE: $Windows.~BT\Sources\Panther\UnattendGC	Contains information about actions during the OOBE phase.	Investigating rollbacks that failed during OOBE phase and operations – 0x4001C, 0x4001D, 0x4001E, 0x4001F.
	Rollback: $Windows.~BT/ Sources\Rollback	Contains information about actions during rollback.	Investigating generic rollbacks - 0xC1900101.
	Pre-initialization (prior to down level): Windows	Contains information about initializing setup.	If setup fails to launch.
	Post-upgrade (after OOBE): Windows\Panther	Contains information about setup actions during the installation.	Investigate post-upgrade related issues.
setuperr.log	Same as setupact.log	Contains information about setup errors during the installation.	Review all errors encountered during the installation phase.
miglog.xml	Post-upgrade (after OOBE): Windows\Panther	Contains information about what was migrated during the installation.	Identify post upgrade data migration issues.

BlueBox.log	Down-Level: Windows\Logs\Mosetup	Contains information communication between setup.exe and Windows Update.	Use during WSUS and WU down-level failures or for 0xC1900107.
Supplemental rollback logs: Setupmem.dmp setupapi.dev.log Event logs (*.evtx)	$Windows.~BT\Sources\Rollback	Additional logs collected during rollback.	Setupmem.dmp: If OS bugchecks during upgrade, setup will attempt to extract a mini-dump. Setupapi: Device install issues - 0x30018 Event logs: Generic rollbacks (0xC1900101) or unexpected reboots.

Log entry structure

A setupact.log or setuperr.log entry (files are located at C:\Windows) includes the following elements:

1. The date and time - 2016-09-08 09:20:05.
2. The log level - Info, Warning, Error, Fatal Error.
3. The logging component - CONX, MOUPG, PANTHR, SP, IBSLIB, MIG, DISM, CSI, CBS.

The logging components SP (setup platform), MIG (migration engine), and CONX (compatibility information) are particularly useful for troubleshooting Windows Setup errors.

4. The message - Operation completed successfully.

Several log files are created during each phase of the upgrade process. These log files are essential for troubleshooting upgrade problems. By default, the folders that contain these log files are hidden on the upgrade target computer. To view the log files, configure Windows Explorer to view hidden items, or use a tool to automatically gather these logs. The most useful log is setupact.log. The log files are located in a different folder depending on the Windows Setup phase. Recall that you can determine the phase from the extend code.

Log files

-https://docs.microsoft.com/en-us/windows/deployment/upgrade/log-files