Filename: microsoft-ms101-4-3-1-analyze-upgrade-readiness-for-windows-10-know
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Plan Windows 10 Deployment
EpisodeName: Analyze Upgrade Readiness for Windows 10 - Know
Description: Adam and Wes discuss what you need to know to successfully analyze upgrade readiness for Windows 10.

Analyze Upgrade Readiness for Windows 10 - Know

Implement Modern Device Services (30-35%)

Plan Windows 10 Deployment
• Plan for Windows as a Service (WaaS)
• Plan the Appropriate Windows 10 Enterprise Deployment Method
• Analyze Upgrade Readiness for Windows 10
• Evaluate & Deploy Additional Windows 10 Enterprise Security Features

==========

Analyze Upgrade Readiness for Windows 10 - Know

With Windows diagnostic data enabled, Upgrade Readiness collects system, application, and driver data for analysis. Microsoft then identifies compatibility issues that can block an upgrade and suggests fixes.

NOTE: For system, application, and driver data to be shared with Microsoft, you must configure user computers to send data.

Data collection -

Windows 10 and Windows Server includes the Connected User Experiences and Telemetry component, which uses Event Tracing for Windows (ETW) tracelogging technology that gathers and stores diagnostic data events and data.

Operating system features and some management applications are instrumented to publish events and data.

Events are gathered using public operating system event logging and tracing APIs.

NOTE: You can configure the diagnostic data level by using MDM policy, Group Policy, or registry settings.

The Connected User Experiences and Telemetry component transmits the diagnostic data.

Data transmission -

All diagnostic data is encrypted using SSL and uses certificate pinning during transfer from the device to the Microsoft Data Management Service.

Real-time events, such as Windows Defender Advanced Threat Protection, are always sent immediately.

Normal events are not uploaded on metered networks, unless you are on a metered server connection.

On a free network, normal events can be uploaded every 4 hours if on battery, or every 15 minutes if on A/C power.

Diagnostic and crash data are only uploaded on A/C power and free networks.

The data transmitted at the Basic and Enhanced data diagnostic levels is quite small; typically less than 1 MB per device per day, but occasionally up to 2 MB per device per day.

Configure the diagnostic data level -

You can configure your device's diagnostic data settings using the management tools you are already using, such as Group Policy, MDM, or Windows Provisioning.

You can also manually change your settings using Registry Editor.

Use the appropriate value in the table below when you configure the management policy.

Level	Value
Security	0
Basic	1
Enhanced	2
Full	3

Supported upgrade paths -

Windows 7 and Windows 8.1

To perform an in-place upgrade, user computers must be running the latest version of either Windows 7 SP1 or Windows 8.1. After you enable Windows diagnostic data, Upgrade Readiness performs a full inventory of computers so that you can see which version of Windows is installed on each computer.

NOTE: Upgrade Readiness is designed to best support in-place upgrades. In-place upgrades do not support migrations from BIOS to UEFI or from 32-bit to 64-bit architecture. If you need to migrate computers in these scenarios, use the wipe-and-reload method.

NOTE: While Upgrade Readiness can be used to assist with updating devices from Windows 10 Long-Term Servicing Channel (LTSC) to Windows 10 Semi-Annual Channel, Upgrade Readiness does not support updates to Windows 10 LTSC. The Long-Term Servicing Channel of Windows 10 is not intended for general deployment, and does not receive feature updates, therefore it is not a supported target with Upgrade Readiness.