Key Concepts - Hosted

https://campus.barracuda.com/doc/86544925/

Barracuda Managed Workplace is designed to let you manage many devices easily, and employs common IT standard organizational practices to do so. Having a good understanding of these from the outset allows you to get up and running quickly.

Devices

Devices in Barracuda Managed Workplace are workstations, servers, printers and infrastructure devices. This includes anything that has an IP address and responds to an ICMP ECHO request. Onsite Manager identifies devices by their IP addresses, MAC addresses, DNS names and names provided via any management protocols available.

Management Protocols

Barracuda Managed Workplace collects information about computer networks using a wide variety of technologies, but chief among these are the management protocols Windows Management Instrumentation (WMI) and Simple Network Management Protocol (SNMP). These are used to expose status information about devices to authenticated parties. WMI is available only on Windows operating systems and SNMP is commonly available on routers, firewalls and printers, but is also available on almost all operating systems including Windows.

Website

Barracuda Managed Workplace can also monitor websites in addition to IP-based devices. Onsite Manager performs the monitoring, so the websites can be on the Internet or local to the client's network.

Site

A Barracuda Managed Workplace site is a logical container for devices and websites. Most typically this will be a single physical location for one of your clients, but may also be multiple locations using Device Managers.

Monitors

Monitors are rules for sampling information from a device, applications running on a device or website. The rules define what data should be collected, when to collect it and how frequently it is sampled. The following types of monitors are available:

- Device Availability
- Device Warranty
- Bandwidth
- Windows Events
- Performance Counters
- Windows Services
- Print Services
- Mobile Device
- Network Services
- SNMP
- SNMP Traps
- Syslog Messages
- Website availability, performance and content search
- AMT Events
- Patch Status
- MBSA Reports
- SCE
- Custom log Content

Alerts

Alerts are an event that is triggered when data being monitored crosses a user-defined threshold. Alerts are displayed on the Central Dashboard in Service

Center, but can also be configured to generate an email, create a trouble ticket or both. Alerts for some monitor types can be configured to self-heal, which means they automatically clear when the condition causing the alert is no longer true.

Groups

Groups are containers that allow you to manage many similar devices. You can apply monitoring policies, run automated tasks and generate reports at the group level. There are two kinds of groups

you can create:

- Service groups contain devices from one or more client sites and can be used to manage similar devices across multiple sites.

Site groups contain only devices from a single site and can be used to manage devices on one site only. Some groups may be preconfigured for use by your hosting provider.