Glossary

https://campus.barracuda.com/doc/84314207/

Glossary

Active Management Technology (AMT) Technology developed by Intel® included with vPro™ chips, that provides Managed Workplace with the ability to capture system board level events and remotely power cycle devices.

Alert The notification used to inform operators of Managed Workplace that data being monitored is in a user-defined state. Alerts appear on the Central Dashboard and Alerts Viewer for Service Center, and may additionally trigger email notifications or trouble ticket creation. Some types of alerts can clear themselves, or self-heal, when the condition no longer exists.

Alert Actions Alert actions are automated processes that can be set for each alert configuration. The available actions include creating a trouble ticket, self-healing when the condition no longer exists and running a script.

Alert Category Organizational units for the presentation of alert indicators on the Central Dashboard. Alert categories can also be used to add specificity to reporting and alert schedules. Alert categories are automatically added to the Central Dashboard when monitoring policies that use them are imported.

Alert Notifications Alert notifications are rules set in each alert configuration that define who is contacted when the condition occurs, and by what means.

Alerts Viewer Designed for network operation centers' wallboards and displays and prioritizes alerts in real-time as they appear on the Central Dashboard. Audible cues can be configured to notify operators that new alerts have arrived.

Application Programming Interface (API) The Managed Workplace API allows qualified Partners with programming resources to inter-operate with Service Center, describing the methods and calls used to insert or extract data from the database via a web service.

Approval Group Approval groups are used only with Patch Management so that Microsoft updates can be approved for multiple devices at once. We recommend that approval groups be organized by operating system type.

Authentication Authentication is when an identity is proven to a network application or resource. This is usually handled either through credentials, such as a username and password pair, or a cryptographic operation, such as using a private and public key pair. In Managed Workplace, users

authenticate their identities with login credentials to Service Center. Authentication also takes place between Onsite Manager and Service Center when communications occur, with or without the use of Secure Sockets Layer certificates.

Central Dashboard The primary display for alerts in the Service Center interface, the Central Dashboard organizes alert indicators by sites, groups, and alert categories.

Data Point A data point is the measurement of the status of a device or application for a single sample. The frequency at which the samples are taken is referred to as the polling interval.

Device A unique responding hardware device Onsite Manager identifies on a network.

Device Alias A user-input identifier for a device. We recommend using device aliases so Service Center users can easily identify devices. This is especially true on networks where the discovered names of devices are very similar due to a strict DNS naming convention.

Device Manager The functional equivalent of Onsite Manager but monitors and manages a single device only. There is a database, but it is bundled with the lightweight application.

Discovered Name The identifier that Onsite Manager assigns to a device it discovers on a network, the discovered name is taken from DNS, the device host name or the sysName.0 OID.

Domain Name System (DNS) A system by which IP addresses are matched to friendly host names. DNS will need to be accessed to create host name records so that the URLs used to access Managed Workplace may be resolved.

Dynamic Host Configuration Protocol (DHCP) A protocol used by networked computers to automatically receive IP addresses and corresponding networking information, such as the Internet Gateway and Subnet Mask.

Escalation Notification A setting in each alert configuration that allows operators to define who to notify when an alert condition has gone unresolved for a predetermined length of time.

Foundation Technology Managed Workplace integrates with a number of Microsoft applications for its core functionality, including ASP.NET, IIS, SQL Server, MBSA and WSUS. These are referred to as the foundation technologies.

Groups Groups are organizational containers against which monitoring policies are applied. There are two types: service groups and site groups.

Hypertext Transfer Protocol (HTTP) A protocol used to transport data over networks, primarily the Internet.

Internet Control Message Protocol (ICMP) A protocol used by Managed Workplace to determine whether devices are able to respond to an ICMP ECHO request, which defines whether the devices are considered Up or Down.

Internet Information Services (IIS) Microsoft's web server, which also handles mail and news. Managed Workplace uses IIS to host various websites, services and application pools, and can use the built-in virtual SMTP mail server.

Internet Protocol (IP) A protocol used for communications across packet-switching internetworks.

Internet Security and Acceleration (ISA) Microsoft's stateful packet and application layer firewall, which also handles Virtual Private Networks and Web Caching (proxy server).

Managed Device A managed device is one from which Onsite Manager is collecting information. To collect as much information as possible, and to enable all features of Managed Workplace, either WMI or SNMP management protocols need to be enabled. Managed devices running a Windows operating system can have both management protocols enabled.

Management Information Base (MIB) A collection of objects (OIDs) in a (virtual) database used to manage devices on a network. MIB files may be used when creating monitors in Service Center.

Media Access Control (MAC) A unique identifier for a network adapter. Managed Workplace uses the MAC address as part of the evidence to identify unique devices.

Microsoft Baseline Security Analyzer (MBSA) A utility that audits the security on Windows operating systems and applications. Onsite Manager by default will run MBSA scans against all Windows devices on a network once a week.

Microsoft Desktop Engine (MSDE) A free, scaled-down version of Microsoft SQL, with a 2 GB database size limit. This has been replaced by Microsoft SQL 2005 Express, which has a 4 GB database size limit. Onsite Manager may use either of these to host its database (MWData). SQL Express is included with the Onsite Manager installer.

Monitoring Policy A monitoring policy is a collection of monitors and associated alert rules for a specific application or hardware device. We provide an ever-growing library of predefined monitoring policies delivered with each release, and makes new monitoring policies available in the Update Center as they are created.

Network Services Applications requiring open TCP ports that Onsite Manager is able to monitor. A default list of the most common network services are automatically scanned and discovered, but custom network services may also be added through Service Center.

Object Identifier (OID) A unique object listed in the Management Information Base (MIB) for a

Device.

Onsite Manager (OM) Onsite Manager is the component of Managed Workplace installed on remote networks to collect monitoring data, run scripts, route remote control sessions and deploy software updates.

Patch Management A Managed Workplace feature that integrates with servers at remote sites to centralize their management. This allows Partners to approve and install Microsoft updates to a wide variety of operating systems and applications.

Performance Counter Performance Counters represent data on specific aspects of a system or service. Monitoring of performance counters is one of the primary means of collecting information about Windows devices in Managed Workplace.

Polling Interval A monitor's polling interval is the frequency with which the status of the monitored device or application is sampled. Each sample that is taken is referred to as a data point.

Ports The Transport Layer Protocols TCP and UDP use identifiers called ports to logically separate services from one another. Access to certain ports by direction (inbound or outbound) can be configured in firewalls and other network infrastructure devices.

Professional Services Automation (PSA) Systems PSA systems are used to manage the delivery of client projects, and the resources that are required for those projects, such as skilled personnel and equipment. In addition to project management, other typical functions include time recording, billing, and reporting. Managed Workplace can integrate with Salesforce, Autotask, ConnectWise, Tigerpaw, and others.

Proxy Server A server that allows clients to make indirect network connections to other networks. Onsite Managers can be configured to communicate with Service Center through a proxy.

Remote Desktop Protocol (RDP) The protocol used to connect remotely to Microsoft Terminal Services. Client software is included with all modern

versions of the Windows operating system (those released following Windows 2000).

Secure Shell (SSH) A protocol that uses public-key encryption to establish a secure remote connection to a device. Managed Workplace uses the PuTTY client application to establish these connections.

Secure Sockets Layer (SSL) A cryptographic protocol that provides secure communications over internetworks for data transfers by confirming the identity of the connected devices. SSL may optionally be used to secure the web pages used for the communications and operations of Managed

Workplace.

Service Center (SC) Service Center refers to both the centralized database and application servers that collect incoming monitoring data from remote networks and also the user interface that operators use to view and manipulate the data.

Service Center Monitor A Windows service installed on the Service Center application server that receives the monitoring telemetry from Onsite Managers.

Service Group The recommended organizational container for devices in Managed Workplace, which may contain devices from multiple sites. The advantage of service groups comes from the ease of administration they offer when managing like devices or applications.

Simple Mail Transfer Protocol (SMTP) The favored protocol used for email transmission. Managed Workplace makes use of an SMTP server to send email alerts.

Simple Network Management Protocol (SNMP) A protocol used to monitor devices for conditions requiring attention. An implementation of SNMP is available for most operating systems, and most hardware devices make use of this protocol to report status. SNMP is the primary means by which Managed Workplace monitors network devices and non-Windows operating systems.

Site Group An organizational container for devices related to a single customer site. The advantage to using site groups comes from the ease of identifying alerts occurring on a per-site basis, and they also provide a means by which you can easily apply monitoring policies for customers with unique requirements.

SNMP Trap A message sent from an SNMP-enabled device, advising of a condition being present on the device. Onsite Manager is an SNMP Trap receiver, and must be configured as such in the SNMP-enabled device to capture the SNMP Traps sent out.

SNMP-enabled Devices are considered to be SNMP-enabled when configured with a community string that is listed in the Onsite Manager network scan. Matching community strings allows Onsite Manager to query the status of the devices using the SNMP protocol. Hardware devices, most operating systems and applications can all report status using SNMP.

Structured Query Language (SQL) A computer language used to perform operations against a database. Managed Workplace requires Microsoft SQL Server 2000/2005 be used to house the Service Center database (SCData). Onsite Manager may be housed on Microsoft SQL Server 2000/2005, or the stripped down free versions, MSDE (Microsoft Desktop Engine) or SQL 2005 Express.

Subnet A subnet is a partitioned range of logical addresses (IP addresses).

Syslog A protocol and standard used for sending status messages between devices on an IP network.

Onsite Manager is a syslog receiver and by default captures all syslog messages sent to it.

Telnet A client/server protocol that is implemented in Managed Workplace remoting. This may be used to remote into devices that are configured as a Telnet server.

Transmission Control Protocol (TCP) A transmission protocol that exchanges streams of data from sender to receiver in a connection full session. This is the primary protocol used to transport information from Onsite Manager to Service Center.

Trouble Ticket A trackable list of notes for a specific issue that has occurred. Tickets may be created as alert actions or manually, and may also be synchronized with third-party (Professional Services Automation (PSA) systems.

Uniform Resource Locator (URL) A uniform syntax used to locate resources over a network.

User Datagram Protocol (UDP) A connectionless protocol, typically used to broadcast messages over a network.

Virtual Network Computing (VNC) A client/server desktop sharing suite that makes use of the RFB protocol. Managed Workplace supports any VNC implementation being used to establish remote sessions.

Virtual Private Network (VPN) A means of creating a private network communicating over a public network.

Virtual Service Center (VSC) A Service Center used by a Partner that is not installed on their premises, but is instead made available by a Managed Workplace hosting provider.

Windows Events Windows Events are information events recorded in Windows log files that may be read using the Event Viewer. Managed Workplace monitors Windows Events for definable conditions, and generates alerts when the conditions are discovered on a device.

Windows Management Instrumentation (WMI) A component of the Windows Operating System that is used as an interface through which operating system components can provide information and notifications. WMI is the primary means by which Managed Workplace retrieves information about Windows devices.

Windows Remote Management (WinRM) Microsoft’s implementation of WS-Man.

WMI-enabled Devices are considered to be WMI-enabled when Onsite Manager has the ability to query the technology for status updates. Only Windows devices can be WMI-enabled.

WS-Management (WS-MAN) - A management system based on open DMTF and Internet standards that provides a common way for systems to access and exchange management information over a networked infrastructure. Managed Workplace accesses WMI over WS-MAN when it is available on a device.