

10 Most Common Desktop Management Issues

Content:

10 Most Common Microsoft Desktop Infrastructure Management Issues	4
1. Dynamic Security Patch Management.....	4
2. Hardware Inventory	5
3. Software Inventory and License Compliance.....	5
4. Software Application Usage and Consolidation	6
5. Automated Application Deployment.....	6
6. Operating System Upgrade Compatibility	6
7. Operating System Image Creation.....	7
8. System Reporting.....	7
9. Managing the Laptop Environment	7
10. PC Remote Control	8

Document Management

Document Control

This material and any part of its contents are the property of, and proprietary to, Eurodata Systems Plc. Without the express written consent of Eurodata Systems Plc, this material is not to be disclosed, duplicated or used, in whole or in part, for any purpose other than evaluation. This material shall be kept in a safe place at all times and shall be returned to Eurodata Systems Plc upon request.

Contact Information

Eurodata is number one for Microsoft solutions and is one of the few companies to obtain the prestigious level of Microsoft Gold Certified Partner.

You benefit directly from our 10-year relationship with Microsoft through in-depth access to exclusive resources and early product information. To keep you up to date with current and new Microsoft technologies, we hold regular customer briefings and we use the sophisticated Eurodata Systems test lab to evaluate Microsoft Beta software.

For further information on our Microsoft Solutions portfolio please go to www.eurodatasystems.com or call 020 7619 1500.

10 Most Common Microsoft Desktop Infrastructure Management Issues

Based on his experience with Microsoft infrastructure management solutions, David Morgan has identified the following 10 most common desktop infrastructure management issues.

These issues can dramatically impact the day-to-day running and management of a desktop environment and can be avoided with the introduction of proactive measures; corrective steps are advised in each case.

1. Dynamic Security Patch Management

With the recent push by Microsoft to increase the security of their applications, organisations need a strategy for rapidly assessing and applying product updates as they become available. However, most companies still employ a wholly reactive and ad-hoc approach to managing updates, with patches often being applied manually to PCs in an inconsistent manner. Such a strategy is no longer viable in an age in which the flow of software updates is constant and the threat of malicious attack is ever present.

According to McAfee, over 15,000 new threats were added to its database in the first nine months of 2004 and at the same time the company announced that it had detected its 100,000th malicious threat¹. Many of these threats exploit security vulnerabilities in Microsoft software and consequently both McAfee and Microsoft recommend that all organisations stay up to date with the latest security patches. Clearly, all organisations require a dynamic patch management strategy to allow them to proactively manage updates to their desktop infrastructure.

Microsoft provides two solutions to assist in the creation of a dynamic patch management strategy for both Microsoft operating systems and applications.

One of the most advanced products that address this issue is Microsoft's System Management Server (SMS) 2003. This fully integrated desktop management system provides a high degree of flexibility and functionality in targeting and scheduling the deployment of security updates to clients and servers. Deadlines can be specified to ensure that patches install only during designated update timeframes or complete by a specific date and time. Updates can also be targeted to specific machines based on their hardware or software configurations. SMS uses a security scan tool installed on the PCs to provide on-demand compliance checks for updates. The SMS server can then be used to download the required patches from the Microsoft website and deploy them to only the vulnerable PCs that meet the deployment criteria specified. It is then possible to report on the progress of the deployment and the current patch state of the PCs. This solution offers an integrated and proactive solution to the patch management issue.

For smaller networks that typically have less technical expertise available, Microsoft provides a simpler product to address the patch management task: Windows Server Update Services (WSUS) uses one or more servers to store Microsoft updates before they are authorised and scheduled for deployment by an administrator. WSUS makes use of an Automatic Updates software component on each Microsoft client. This approach provides limited, machine-based targeting and only basic scheduling functionality.

1

http://www.mcafeesecurity.com/us/about/press/mcafee_enterprise/2004/20040920_085956.htm

2. Hardware Inventory

It is important to keep an accurate record of the type and quantity of hardware deployed across a network. An accurate hardware inventory aids hardware rationalisation, ensures no unauthorised hardware reconfiguration occurs and can help demonstrate contractual obligations are being met. Failure to accurately keep these records can lead to increased costs for both support and hardware purchasing, as it may lead to an inefficient allocation of resource or erroneous deployment of software to hardware that is not fit to run particular applications.

Hardware inventory should be gathered and maintained automatically; manually recording hardware details is an onerous task to carry out and it can also prove to be very difficult to ensure accuracy is maintained on an ongoing basis.

Microsoft's solution to this problem is the provision of a customisable hardware inventory component as part of its SMS 2003 application. This component integrates with Windows Management Instrumentation (WMI) to provide over 100 computer system hardware features such as physical memory and hard-disk drive configuration. In addition, SMS can also inventory numerous operating system details including version and service pack level, as well as logical drive and pagefile configuration.

Using this detailed information, organisations can easily and quickly fulfil their hardware asset management requirements without resorting to regular, manual audits of the PCs. A cost saving can therefore be achieved by using SMS to increase the accuracy of audits and remove the need to regularly dedicate resources to manual hardware auditing.

3. Software Inventory and License Compliance

It is always important for the IT department to know exactly what software is installed on the PCs in their environment. If software is not audited it is almost impossible to comply with license agreements and ensure that no unauthorised software has been installed which may breach company policies.

License compliance is one of the most pressing issues for infrastructure managers today. Due to the financial penalties levied on companies who fail to ensure compliance, many organisations need instant and up to date information on their installed application base.

In order to ensure license compliance, many organisations regularly audit their PCs for licensed software to ensure they have enough licenses, and purchase any additional ones as required. Using this method alone, however, there is the possibility that a period exists between audits when license compliance is not achieved and therefore financial penalties may be incurred.

In response, Microsoft provides a customisable software inventory component as part of its SMS 2003 application. This component scans PC hard-drives and returns a complete list of all applications installed. Utilising this tool, the IT department can quickly, accurately and remotely collect and maintain software asset information. This functionality allows monitoring of the applications that are installed, the number of instances of these applications, and whether any unauthorised software is present. In this way the need for manual software audits is removed, the likelihood of user error is limited, and the risk of financial penalties being levied is substantially reduced.

4. Software Application Usage and Consolidation

An issue that is related to licence compliance is that many organisations are unaware of how software is actually used within the company. A consequence of this is that companies tend to hold more licences for some applications than are actually required. Often, users may request an application for a specific reason and then only use the software for a short period or not at all. However, if software use is not metered, this lack of use is not detected and so unused applications are never uninstalled. This has cost implications for organisations if licenses are purchased that are not necessary.

With the ability to actually meter the usage of any application, SMS 2003 allows administrators to monitor when particular applications have been run on PCs and the user that has run them. This enables the IT department to record the maximum number of concurrent usage instances for given applications. This functionality allows organisations to save money on potential new application purchases, and effectively phase out unused applications. *Ultimately, organisations want to use only the software that has been paid for and to only pay for software that is used.*

5. Automated Application Deployment

Manually installing software onto PCs can be incredibly time consuming; someone must visit one or more PCs, launch the installation and wait for it to complete before moving on to the next PC. Therefore manual installations take support staff away from their main day-to-day duties, is inherently inefficient, and does not allow for accurate reporting on the progress of installations.

In order to reduce the administrative time and effort required to deploy software, an automated deployment solution should be implemented that can deploy applications simultaneously to multiple PCs.

Application deployment can be completed from a single administrative point using the features and functionality of SMS 2003. SMS offers a greater degree of control over deployment compared with an application deployment that utilises Active Directory group policy objects; SMS allows deployments to be targeted against machines and users based on a wide variety of properties including client network, hardware, and software configurations. In addition, SMS allows for complex scheduling of deployments to ensure that installation occurs only between specified times whereas this is not possible with GPO deployments. This allows applications to be deployed to PCs during periods of low network utilisation, such as overnight, which also reduces the impact on users. In-depth status reporting on progress is also available using built-in and customisable web-based reports.

6. Operating System Upgrade Compatibility

Upgrading to a new Operating System is fraught with difficulties, one of the most critical being the ability to determine the compatibility of the hardware and software deployed in the network. Before embarking on an Operating System upgrade, a test environment should be built and each application thoroughly tested to ensure compatibility in order to avoid incompatibility problems during migration. There can be no substitute for thorough testing as an important phase in any deployment or upgrade project; however there are methods that allow the process to be expedited and to reduce the severity of potential problems.

Microsoft has created a solution called the 'Application Compatibility Toolkit (ACT)' – a set of tools used to simplify the Windows XP migration process. There are two elements involved, **evaluation** and **mitigation**.

The **evaluation** stage uses an automated agent installed on client PCs to retrieve information about the installed applications. If any applications are not compatible, then

the **mitigation** tool is employed to attempt to overcome the issues by using its database of common compatibility problem fixes. This can help to resolve a large number of application issues that could otherwise impact on the time-scales of the upgrade or even jeopardise the entire project. The ACT toolkit therefore not only allows potentially problematic applications to be identified but also helps resolve issues before continuing with the upgrade project.

7. Operating System Image Creation

Many organisations maintain a standard operating system image that is used as a template that can be used to quickly distribute an Operating System and set of applications to end users. By capturing an Operating System and applications together in an image, the time taken to initially prepare a PC or to recover when a PC fails is drastically reduced. There are many applications that can be used to create and rollout these images along with applications, the most notable being Symantec Ghost and PowerQuest PQI.

Microsoft has now created an imaging application called the Operating System Deployment (OSD) feature pack, which integrates into SMS 2003 and can therefore leverage an organisation's existing SMS 2003 infrastructure.

The OSD feature pack is capable of compressing images with a high compression ratio that reduces an image size by approximately 3:1, therefore reducing the network bandwidth used when deploying the image. This image file is stored on an SMS distribution point and can be targeted to both existing PCs in the SMS system as well as new PCs that are later added to the network. It is also possible to create *unattended installations* that can, among other things, rename the PC and install additional applications based on the PC name, IP address, or even the department it was installed in. This removes the need for the SMS administrator to target additional departmental applications to new PCs installed on the network.

Eurodata Systems advises that organisations who have or are considering implementing SMS, should also consider employing the OSD feature pack in order to take advantage of the high degree of automation and flexibility this product affords.

8. System Reporting

Increasingly, IT departments are required to produce reports that demonstrate the status of security patch distribution, application deployments, hardware changes and other services provided. In order to create these reports it is often necessary to correlate data from multiple sources, which in turn are often exported into spreadsheets for viewing. This is time consuming and diverts IT support staff from the day to day running of the network.

If SMS 2003 has been implemented as the organisation's management solution, all the information that has been collected is available in a single location and reports can be generated quickly and simply. The web-based format of these out-of-the-box reports makes them easy to view and to share with others. The central nature of this reporting system saves time and allows the IT department to focus on key tasks.

9. Managing the Laptop Environment

Laptops provide unique challenges to IT support staff. By their very nature they could be connecting to different networks in different locations for only short periods of time. This presents challenges when considering how to implement a patch management and application deployment strategy for these users. Many organisations therefore request that laptops are brought into the support office to be patched and have new applications deployed. However, as this requires that both the laptop owner and the support team set aside time for this process, it is one of the most inefficient support processes undertaken.

This situation also presents security risks in that there are typically lengthy periods when laptops are not being updated with the most recent security patches.

The problem that must be addressed when considering how best to serve laptop users is that laptops typically connect to a corporate network over very limited bandwidth connections. To overcome some of the deployment problems this causes, Microsoft has integrated into SMS a technology called Background Intelligent Transfer System (BITS). When more important network tasks are being carried out, such as data synchronisation, e-mail transmission or Internet browsing, BITS limits the bandwidth used by any software or security update application in order to free up the bandwidth for these foreground tasks. However, during times when bandwidth is not being demanded by other applications, BITS will allow greater bandwidth to be allocated to the update task.

BITS also employs *checkpoint restarts*, so if the laptop loses connectivity before the download completes it will restart from that point with no loss of data. This more efficiently utilises the limited available bandwidth by eliminating the need to resend data that the laptop has already received.

10. PC Remote Control

The ability for support staff to gain remote control over client PCs presents the opportunity to diagnose and resolve problems without the need to visit the end user. The IT support team can then rapidly troubleshoot problems and attempt to resolve these without requiring user input.

Microsoft has integrated two remote access and control tools into Windows XP, 'Remote Assistance' and 'Remote Desktop'. Remote assistance allows a user's *active* session to be monitored and controlled, whereas remote desktop allows a new logon session to be made onto a user's PC.

Windows 2000 has no built-in remote control functionality. However, this can be provided for by using the 'remote tools' component of SMS. In this scenario, the SMS remote control agent is enabled on the client PCs and it then provides the functionality to monitor and control a user's active session in a similar manner to XP's Remote Assistance tool.

About Eurodata Systems Plc

Eurodata Systems has become one of the few truly end-to-end service providers. Established in 1990, the company is now a mature business with more than 100 highly-skilled technical professionals offering solutions across the complete IT spectrum from network audit to full network security.

The company's end-to-end capability allows clients to pick and choose from an unrivalled range of skill sets and expertise. A single point of contact saves you time, effort and money, eliminating the problems of dealing with multiple service providers, warranties and agreements.

Eurodata Systems develops and implements comprehensive IT strategies and integrated business solutions to help organisations make a successful transition to new technology.

As one of only a few IT services companies to achieve the prestigious dual competency status of Microsoft Gold Certified Partner for Advanced Infrastructure and Networking Infrastructure Solutions. With years of experience in designing, implementing and supporting complex Microsoft environments Eurodata Systems has a complete end-to-end understanding of these world-leading applications, and advise our clients on how they can gain maximum business benefit through their professional implementation and management.

Eurodata System offers core services for the following solutions:

- Operating System Migration.
- Active Directory Design.
- Messaging and Collaboration Solutions.
- Mobile Solutions.
- Security.
- Ongoing Support.
- Management Solutions.

Proven Project Methodology

Successful change means, identifying the processes that will transform organisational performance; gain the commitment of people; and develop the right technology solution. Our "People, Process and Technology" approach ensures an effective environment for change.

Eurodata Systems delivers business benefit to clients through its close working partnership with Microsoft, an in-depth knowledge of the Microsoft Infrastructure solutions technology and a refined implementation methodology developed over many years. This tried and tested methodology ensures a smooth and seamless upgrade minimising any business disruption, from concept through to solution delivery and support. Eurodata Systems will manage your solution through four phases:

- **Analysis**
- **Design**
- **Implementation**
- **Review**

Eurodata Systems comprehensive planning process will establish a sound definition of the work to be performed and generate a solid understanding of the commitments to be undertaken.

As always the focus is on the business enablers of the technology, rather than a technical functionality. Deployment projects are always driven by commercial needs.

By offering a high level of continuity throughout the project – the same personnel involved from the beginning of the tender process will remain throughout the entire project – Eurodata Systems can ensure that your commercial goals are realised.

The team's methodology includes proven risk minimisation techniques incorporated into the management of each of the complex elements that make up a project. These include:

- **Maintenance of an effective customer relationship**
- **Leadership of a productive and motivated project delivery team**
- **Focusing on quality management and quality assurance**

Eurodata Systems draws on more than 15 years' experience of delivering IT solutions to ensure each migration project is completed smoothly and successfully. The company's Consultancy and Engineering teams comprise of IT professionals with multi-faceted skills as well as industry and professional accreditations that span numerous disciplines. Knowledge transfer is an essential part of the migration project – by ensuring clients have the appropriate post installation knowledge, skill set and system management capability.

Eurodata Systems complete end-to-end migration expertise includes:

- **Flexible, scalable and manageable solutions**
- **A tried and tested migration methodology**
- **A focus on delivering business benefits, not just technological functionality**
- **Tailored support contracts to meet clients' precise needs**
- **Automated and escalated helpdesk facility**
- **Microsoft Gold Certified Partner for Advanced Infrastructure and Networking Solutions with access to Microsoft resources and early product information**

Eurodata Systems commitment to its clients does not end when implementation is complete. The importance of continuous support is underlined with a comprehensive portfolio of end-to-end services designed to give you flexible support whenever you need it.

Partnerships and Accreditations

Eurodata Systems have built strategic relationships with all the leading IT vendors and have achieved some of the industry's toughest accreditations, so you can be confident of receiving qualified, independent technical advice.

Some of Eurodata Systems key partnerships and accreditations include:

- **Microsoft Gold Certified Partner for Advanced Infrastructure, Networking Infrastructure Solutions and Security Solutions.**
- **HP Enterprise Partner**
- **Cisco Elect and Premier Partner**
- **Whale Communications Master Partner**

- **Check Point Consulting Partner**
- **CHECK Accredited**
- **ISO 9001 compliant**

Further Information

Working with our clients, we have found more and more the need for precise and relevant information that is easy to digest whether you are a non technical business decision maker or an IT Director who doesn't have the time to wade through mountains of technical and business links on new Microsoft technologies.

For these reason we have developed a number of precise information guides, please visit our website for further information. www.eurodatasystems.com