ERNW
providing security.

Friedwa
rt Kuhn

Digital unterschrieben von Friedwart Kuhn
DN: c=DE, o=ERNW Enno Rey Netzwerke GmbH, cn=Friedwart Kuhn, givenName=Friedwart Nikodemus Michael, sn=Kuhn, serialNumber=DTRWM3841760 41574922
Datum: 2015.02.11 19:19:59 +01'00'

ERNW Newsletter 47 / February 2015

High-level Security Concept for End-of-life Windows Servers

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4

69115 Heidelberg

Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de

Version: 1.0

Date: 2/11/2015

Author(s): Friedwart Kuhn, Christopher Werny, Dominik Phillips, Heinrich Wiederkehr

ERNW
providing security.

Table of Content

1 Introduction

This newsletter gives recommendations to continue the operation of servers/services, which are announced End-of-Life (EOL) from the vendors, in a secure manner. The primary goal should be always to decommission or migrate the majority of EOL Windows servers to OS versions, supported by the vendor. However, it must be considered that a number of servers cannot be migrated or shut down and must remain operational and accessible. Thus, the arising question is, whether and how security risks might be addressed in a feasible manner in order to guarantee an acceptable risk level for EOL servers. With the recommendations given in this document, which is a high-level security concept for EOL Windows servers, the remaining risk might be reduced to an acceptable level.

2 Scope of the Security Concept

The present high-level security concept for the EOL Windows servers, covers the following areas:

- Identification and evaluation of relevant risks of operating EOL server environments.
- Guidelines for the design of a secure EOL environment, including the areas:
  - Network design.
  - Virtualization design.
  - Active Directory design.
- Guidelines for the development of a secure administration model for EOL server environments.
- Guidance for the secure operation of Domain Controllers and EOL servers.
- Security monitoring and logging recommendations.

The focus of the security concept is mainly on Windows server system, nevertheless, general recommendations can be applied to platforms with other operating systems. Furthermore, applications installed on the EOL server systems are not in the scope of this document, although basic guidelines are given (see section 7.2).

3 Assessing Threats and Vulnerabilities in EOL Server Environments

Operating server systems with an OS, for which vendor support has ended, comes with many risks that have to be considered and addressed. The biggest challenge posed by this undertaking is managing the missing security updates for potential vulnerabilities, arising after the vendor stopped releasing patches. As these issues will not be addressed by official means[1], attackers will always have an advantage over the enterprise's server operators.

This leads to the following relevant threats:

- Potentially persistent vulnerabilities with a potentially high number of exploits.
- Working exploits are supposedly delayed until support ends, ensuring a big enough time frame for a successful attack.
- Current security updates can be reverse engineered, revealing vulnerabilities in End-of-Life operating systems.
- End-of-support systems are more prone to exploits in itself, but they can also be used as a first entry point to strike at other systems.
- Credential theft and pass-the-hash attacks became most recently publicly known and pose a significant threat in Windows environments[2]. In homogeneous network environments, with up-to-date operating systems, this has to be seen as a fundamental threat. The risk is considerably higher, when machines that are running unsupported software are mixed with current systems.
- Higher probability for malware infections, due to potential unpatched vulnerabilities.
- Security relevant incidents can be overlooked, as exploits and vulnerabilities don't become known to the public in a timely manner.
- Anti-malware and anti-virus applications may not support EOL systems.

Corresponding vulnerabilities are:

- An unsupported operating system is a vulnerability in itself, but can also be seen as a catalyst, facilitating other threats.
- End-of-Life systems are mixed with current systems in the same environment. No organisational or technical isolation.
- Separate administration model and corresponding roles are not defined for the administration of EOL servers.
- Usage of outdated third-party applications.
- Missing security monitoring and logging solutions.

Relevant mitigating controls for the associated risks are:

- Strict organisational and technical isolation End-of-Life systems, including filtering technologies.
- Development of a separate administration tier model with well-defined roles.
- Implementation of an appropriate anti-malware and anti-virus solution.
- Implementation of a security monitoring solution.

In this security concept, the relevant mitigating controls for securely operating an EOL server environment, are specified and explained.

---

[1] *Exceptions are possible, but they will be exceptions. See https://technet.microsoft.com/library/security/ms14-021.*
[2] *99% of Active Directory compromises are – according to Microsoft – estimated as being based on pass-the-hash attacks. See* http://channel9.msdn.com/Events/TechEd/NorthAmerica/2014/DCIM-B359#fbid*; minute 10:35.*

4 EOL Server Environment Security Design

4.1 Network Design Considerations

4.1.1 Dedicated IPv4 Subnets for EOL Server

In order to achieve an efficient and effective filtering approach for the EOL servers in the dedicated Active Directory forest, it is necessary to group the EOL servers in dedicated IPv4 subnets. These subnets shall be allocated from the already used address range. This logical grouping, as already mentioned, allows to easily identify EOL servers (based on the IPv4 prefix) which improves the operational feasibility in regards to logging, monitoring and filtering the traffic from/to these servers.

4.1.1.1 Datacenter

It is recommended to reserve at least one /23 IPv4 (split into two /24) subnet in each datacenter location. Depending on the specific amount of EOL servers it may be necessary to increase the subnet size to a /22 or even a /21 (which are then split into the corresponding amount of /24). The exact number has to be evaluated. Even though the EOL servers could reside in a single large layer 2 broadcast domain it is recommended to use /24 as the maximum subnet size. This will ensure that the broadcast domain does not get too big (and thereby decreasing the attack surface of the systems[3]) and also allows the filtering of traffic between those segments (if necessary).

4.1.1.2 Sites

It is recommended to reserve at least one /24 IPv4 subnet in each site where EOL servers are currently in production. As with the datacenter, it may be necessary to reserve more than one /24 subnet depending on the amount of EOL servers in a given site.

4.1.2 Filtering of Traffic between the Forests

Through the logical grouping of the EOL servers in distinct IPv4 subnets and subsequently implementing a separate Active Directory forest for these servers, filtering of traffic between those forests can be achieved with reasonable operational effort. This filtering must be implemented as the exposure and threat potential of the EOL servers is higher compared to the Windows Server 2008/2012 systems in the main forest. Specifically, traffic originating from the EOL forest to the main forest must be filtered to only allow needed communication. Hence, it is detrimental to evaluate which communication relationship between EOL and "normal" servers is necessary to achieve the desired functionality. In the following section, the needed TCP and UDP ports are listed which must be permitted to allow basic inter-forest traffic. Additionally, any further initiating connections from the EOL servers to systems in the main forest must be considered and permitted in the rule set.

[3] *E.g. against ARP Spoofing attacks.*

4.1.3 Necessary TCP and UDP Ports for Communication between the Forests[4]

4.1.3.1 Windows Server 2003 and Windows Server 2000

The following table summarizes the necessary TCP and UDP ports for inter-forest trust communication between the Domain Controllers in their respective forest.

Source Port	Destination Port	Service
1024-65535/TCP	135/TCP	RPC Endpoint Mapper
1024-65535/TCP	1024-65535/TCP	RPC for LSA, SAM, Netlogon, FRS RPC
1024-65535/TCP/UDP	389/TCP/UDP	LDAP
1024-65535/TCP	636/TCP	LDAP SSL
1024-65535/TCP	3268/TCP	LDAP GC
1024-65535/TCP	3269/TCP	LDAP GC SSL
53,1024-65535/TCP/UDP	53/TCP/UDP	DNS
1024-65535/TCP/UDP	88/TCP/UDP	Kerberos
1024-65535/TCP	445/TCP	SMB

4.1.3.2 Windows Server 2008 and Windows Server 2012

The following table summarizes the necessary TCP and UDP ports for inter-forest trust communication between the Domain Controllers in their respective forest.

Source Port	Destination Port	Service
49152-65535/UDP	123/UDP	NTP
49152-65535/TCP	135/TCP	RPC Endpoint Mapper
49152-65535/TCP/UDP	464/TCP/UDP	Kerberos Password Change
49152-65535/TCP	49152-65535/TCP	RPC for LSA, SAM, Netlogon, FRS RPC
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152-65535/TCP	636/TCP	LDAP SSL
49152-65535/TCP	3268/TCP	LDAP GC
49152-65535/TCP	3269/TCP	LDAP GC SSL
53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
49152-65535/TCP	445/TCP	SMB

[4] *According to http:// support.microsoft.com/kb/179442.*

The rules marked yellow are from the author's point of view problematic. This is due to the dynamic nature of the RPC protocol which is heavily used in Active Directory environments. The initial RPC communication is realised over a well-defined port (135/TCP). The communication partners then negotiate dynamically a port from a large port range which is subsequently used for transporting the RPC related traffic. This issue is further complicated because Microsoft changed the port range from Windows Server 2003 to Windows Server 2008 (as depicted by the tables above). In order to reduce the necessary ports which need to be permitted in the firewall rule set, two approaches have to be evaluated. It is strongly recommended to evaluate both approaches laid out below for efficient filtering.

4.1.4 Restricting Active Directory Replication and RPC Traffic to a Specific Port

It is possible to restrict the dynamic RPC ports negotiated between servers and clients by modifying the Windows Registry on the servers which provide RPC services[5]. It should be evaluated whether this approach can be implemented in order to reduce the needed TCP ports permitted in the Firewall.

4.1.5 Stateful Filtering of RPC Traffic

Another approach for permitting the dynamic RPC ports without allowing them generally in the firewall rule set is the stateful inspection of RPC traffic. In this scenario, only traffic destined to TCP port 135 is allowed in the firewall. When configured for inspection, the firewall will inspect the payload of the RPC traffic to ensure it knows which TCP port is dynamically negotiated between the client and the server, and subsequently opens this port dynamically for the duration of the TCP session. It should be evaluated whether the current firewalls in production are capable of inspecting the RPC traffic and evaluate in a PoC whether the stateful inspection is working as desired[6].

4.1.6 Potential Usage of IDPS Devices

Due to the nature of the EOL servers (that no security updates will be released from Microsoft) it is important to implement mitigating controls to ensure that potential exploits cannot be executed on these servers. A firewall is not suitable for this task, as it is blind in regards to potential attacks on the application layer. An Intrusion Detection and Prevention system has the capability to inspect the traffic for evaluation whether the payload transports potential malware/exploits. It is therefore strongly recommended to evaluate the usage of IDPS devices for mitigating these risks. As the infrastructure is primarily virtualized, we recommend evaluating virtualized editions of IDPS devices[7]. The virtualized approach increases the flexibility of implementing these devices without increasing the overall complexity due to more physical hardware in place.

4.2 Virtualization Design

4.2.1 Dedicated VMware Cluster for EOL Server

It is recommended to operate/migrate the EOL server on a dedicated cluster inside the datacentre, or alternatively on a dedicated ESX host in case the Hypervisor is physically located at a secure site and not centrally managed. The consolidation of these servers into one cluster improves the operational feasibility and visibility, as there are clear boundaries where these servers are physically (and logically) located and further simplifies the filtering approach laid out above. It is not necessary to deploy a separate vSphere vCenter server for centralized management. The vCenter

---

[5] *Detailed information can be found in the following article: http://support.microsoft.com/kb/224196*

[6] *It may be necessary to configure workarounds on the firewall for RPC traffic to flow correctly. E.g. for Cisco ASA see the following article: https://supportforums.cisco.com/document/67706/dcerpc-inspection-asapixfwsm*

[7] *E.g. HP Tipping Point or Cisco SourceFire Products.*

servers currently in use for managing the virtualized environment are sufficient and the dedicated cluster should be integrated into

4.2.2 Hardening of VMware ESX Hosts

It is recommended to apply hardening measures (as already done on the production ESX) for the ESX server hosting the EOL servers. The following table outlines recommendations about hardening steps which should be implemented. Before implementing those, it must be ensured that these measures do not disrupt the production traffic of other ESX hosts managed by the vCenter Server.

Recommended Measure	Explanation	Implementation

Disable unnecessary web interfaces on ESXi host	Unnecessary web interfaces must be disabled. Available interfaces can be determined by execution of the command
	`vim-cmd proxysvc/service_list`
		The following services should be disabled by the commands below:
		Web Access login page:
		`vim-cmd proxysvc/remove_service "/ui" "httpsWithRedirect"`
		Managed Object Browser:
		`vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"`
		Host Welcome login page:
		`vim-cmd proxysvc/remove_service "/" "httpsWithRedirect"`

Configure the ESXi host firewall to restrict access to services running on the host. Invalid or too restrictive policies can result in a denial of service for the hypervisor and hosted services.	The ESXi has an integrated firewall, protecting the host system from unauthorized access. The host firewall is enabled by default and can be configured from the vSphere web client.	See 4.2.2.1 for further details about the recommended rule set.
Ensure that vpxuser auto-password change meets policy.	The vpxuser is created automatically when an ESXi host is attached to a vCenter Server and is used for vCenter Server when managing activities for the host. To ensure that the vpxuser auto-password change meets the company policy, the following configuration steps must be performed:	From the vSphere web client, select the vCenter Server and go to "Administration" -> "Server Settings" -> "Advanced Settings". Set VirtualCenter.VimPasswordExpirationInDays to comply with company requirements. This is explicitly necessary for users not handled by central user management system (e.g. technical users).
Enable lockdown mode to restrict	The ESXi lockdown mode must be	Configuration steps via vSphere web

remote access.	used when the ESXi is managed via a vCenter Server.	client: Select the host then select "Configuration" -> "Security Profile". Scroll down to "Lockdown Mode", click "Edit..." and select the "Enable Lockdown Mode" checkbox. 1) Configure Lockdown Mode will be disabled if vCenter is down or the host is disconnected from vCenter. 2) To allow trusted users to override lockdown mode from the vSphere client select "Configuration" -> "Advanced Settings" on the Software Tab. Select DCUI and set the "DCUI.Access" attribute to a comma separated list of the users who are allowed to override lockdown mode (in order to ensure continuity in case of a vCenter outage). 3) By default only the "root" user is a member of the DCUI.Access list. It is not recommended to remove root from the DCUI.Access list as this will revoke the root user's admin privileges on the host.
Configure Host Profiles to monitor and alert on configuration changes.	Host Profiles should be used for deployment and monitoring of ESXi hosts. Different Host Profiles must be generated for different hardware platforms. As the following configuration files are mainly static and therefore only change on manual interaction, they should be monitored: ■ /etc/vmware/esx.conf ■ /etc/vmware/snmp.xml ■ /etc/vmware/vmware.lic ■ /etc/vmware/hostd/proxy.xml ■ /etc/hosts ■ /etc/motd ■ /etc/openwsman/openwsman.conf ■ /etc/sfcb/sfcb.cfg ■ /etc/syslog.conf ■ /etc/vmware/hostd/config.xml ■ /etc/vmware/ssl/rui.crt	The GUI-based generation of Host Profiles can be achieved in multiple ways (however the ESXi host must be administered through vCenter) and is described at *http://pubs.vmware.com/vsphere-50/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-50-host-profiles-guide.pdf.* For recent versions, the most direct way is to select a cluster/host, perform a right-click and select *Host Profiles*. A compliance check against a certain Host Profile can be configured in the vCenter (which is described at the link as well). For checks of multiple ESX hosts the VMware tool *Compliance*

	■ /etc/vmware/ssl/rui.key ■ /etc/vmware/config ■ /etc/vmware/configrules ■ /etc/passwd ■ /etc/shadow ■ /etc/ntp.conf ■ /etc/inittab ■ /etc/profile ■ /etc/rc.local ■ /etc/resolv.conf ■ /etc/vmsyslog.conf ■ /etc/security/access.conf The size of these files should not change regularly: ■ /etc/vmware/license.cfg ■ /etc/opt/vmware/vpxa/vpxa.cfg ■ /var/log/ipmi/0/sdr_content.raw ■ /var/log/ipmi/0/sdr_header.raw ■ /var/log/ipmi/0/sensor_readings.raw The following files are important logfiles and should be tracked for unauthorized access: ■ /var/log/messages ■ /var/log/vmware/hostd.log ■ /var/log/vmware/vpx/vpxa.log	*Checker for vSphere* is available. For the code-based generation/management of Host Profiles, the vSphere PowerCLI cmdlets must be used (refer e.g. to *http://www.vmware.com/support/developer/PowerCLI/PowerCLI41U1/html/Export-VMHostProfile.html*).
Disable ESXi Shell	ESXi Shell is an interactive command line environment available from the DCUI or remotely via SSH and disabled by default.	It is recommended to not change this setting. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell could only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere client or vCLI/PowerCLI.
Disable Managed Object Browser (MOB)	The managed object browser (MOB) provides a way to explore the object model used by the VMkernel to manage the host; it enables configurations to be changed as well. This interface is meant to be used primarily for debugging the vSphere SDK but because there are no access controls it could also be used as a method obtain information about a	MOB can be disabled in configuration file `/etc/vmware/hostd/config.xml` by setting `<enableMob>` to "`false`".

	host being targeted for unauthorized access. This interface must be disabled.	
Use secure transport for Network File Copy (NFC).	NFC (Network File Copy) is used to migrate or clone a VM between two ESXi hosts over the network and must be appropriately secured.	This can be achieved by ■ enabling proper SSL-encryption for NFC or ■ using a trusted transport path (e.g. a dedicated, isolated network segment).
Use valid certificates for ESXi communication.	The ESXi host must use a valid, trustworthy certificate for all SSL-based services (e.g. HTTPS, VIC port) if it is operated/managed without a vCenter. If it is operated through a vCenter, a valid, trustworthy certificate may be used.	To change SSL certificates refer to VMware KB 2034833 *http://kb.vmware.com/kb/2034833*.

Disable CIM	The CIM agent is the process providing hardware health information and should be disabled if it is not required for operations.	CIM can be disabled via vSphere client by navigating through "Configuration" -> "Advanced Configuration" on the ESXi host. There select UserVars and set UserVars.CIMEnabled=0.
		For disabling CIM via ESXi Shell run the following commands on ESXi host:
		`chkconfig sfcbd-watchdog off`
		`chkconfig sfcbd off`
		`/etc/init.d/sfcbd-watchdog stop`
		To check the current status of CIM agent run the command `/etc/init.d/sfcbd-watchdog status`
		If CIM is necessary for health monitoring, access of administrative users must not be possible.
		If CIM is used by monitoring tools, CIM must stay activated.

Configure centralized logging for all ESXi hosts.	All log files should be exported to a centralized log host.	To configure centralized logging follow the configuration steps below:

		Identify the data store path where you want to place scratch, then login to the vSphere web client, navigating to the host and select "Configuration" -> "Advanced Settings"; navigate to Syslog.global.LogHost. Set the Syslog.global.LogHost to the desired log host, similar to tcp://hostname:514 This parameter must be set for each host. A detailed description can be found at *http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003322.*
Ensure proper SNMP configuration	If SNMP is not being used, it must remain disabled.	The following command disables SNMP (while it is disabled by default): `esxcli system snmp set --enable false` If SNMP is being used, the current configuration can be checked by running `esxcli system snmp get` on the ESXi Shell or vCLI. On configuration of SNMP it must be ensured that: ■ a complex community string is used ■ a secure access restriction on infrastructure and ESXi host firewall (UDP 161) is configured. SNMP must be configured on each ESXi host, which can also be done using Host Profiles. It is recommended to use SNMPv3.

4.2.2.1 ESX Host Firewall Settings

The following table shows the recommendations for the ESXi host firewall settings:

Service	Incoming	Outgoing	Default State	Recommendation	Comment
SSH-Server	TCP 22		Enable	Disabled	SSH disabled due to hardening process.
SSH-Client		TCP 22	Disabled	Disabled	
DNS-Client	UDP/TCP 53	UDP/TCP 53	Enabled	Enabled	
Serial Port		TCP 0-65535	Disabled	Disabled	
NTP-Client		UDP 123	Disabled	Enabled	NTP enabled due to hardening process.
Fault Tolerance	TCP/UDP 8100, 8200, 8300	TCP/UDP 80, 8100, 8200, 8300	Enabled	Enabled	If fault tolerance in place, disabled otherwise.
DVFilter	TCP 2222		Disabled	Disabled	
NFC	TCP 902	TCP 902	Enabled	Disabled	Enabled, if NFC is used.
Secure CIM-Server	TCP 5989		Enabled	Disabled	CIM disabled due to hardening process.
HBR		TCP 31031, 44046	Enabled	Disabled	Enabled, if HBR is used.
WOL		UDP 9	Enabled	Disabled	Enabled, if WOL is used.
Syslog		UDP/TCP 514,1514	Disabled	Enabled	Enabled due to logging directives.
DVSSync	UDP 8301, 8302	UDP 8301,8302	Disabled	Disabled	
CIM-Server	TCP 5988		Enabled	Enabled	Disabled if not used.
Software-iSCSI-Client		TCP 3260	Disabled	Disabled	
NFS-Client		TCP 0-65535	Disabled	Disabled	
DHCPv6	TCP/UDP 546	TCP/UDP 547	Enabled	Disabled	Enabled if DHCPv6

					should be used.
vSphere Client	TCP 902, 443		Enabled	Enabled	
vprobeServer	TCP 57007		Disabled	Disabled	
vCenter Update Manager		TCP 80, 9000-9100	Disabled	Disabled	
vSphere Web Access	TCP 80		Enabled	Disabled	
SNMP-Server	UDP 161		Enabled	Enabled	Disabled, if SNMP is not used.
Active Directory		UDP/TCP 88, 123, 137, 139, 389, 445, 464, 3268, 51915	Disabled	Enabled	Necessary for AD integration
FTP-Client	TCP 20	TCP 21	Disabled	Disabled	
httpClient		TCP 80, 443	Disabled	Disabled	
VMware vCenter Agent		UDP 902	Enabled	Enabled	
vMotion	TCP 8000	TCP 8000	Enabled	Enabled	
Gdbserver	TCP 1000-9999, 50000-50999		Disabled	Disabled	
IKED	UDP 500	UDP 500	Disabled	Disabled	
DHCP-Client	UDP 68	UDP 68	Enabled	Disabled	Enabled if DHCP is used for address distribution.
Serial Port	TCP 23, 1024-65535	TCP 0-65535	Disabled	Disabled	
CIM-SLP	UDP/TCP 427		Enable	Enable	Disable if not used for hardware monitoring.

4.2.3 vSwitch Configuration

Due to the already large deployment of the Cisco Nexus 1000v as replacement for the standard vSwitch, it is recommended to implement the virtualized switch for the dedicated EOL clusters. In the case that only the standard vSwitch can be used it is strongly recommended to deactivate the following vSwitch features:

- Promiscuous Mode
- MAC Address Changes
- Forged Transmits

For troubleshooting purposes, it may be necessary to activate the Promiscuous Mode on the vSwitch temporarily. It must be ensured that this mode will be deactivated if it is not needed anymore. Depending on the functionality of a virtual machine, it may be necessary to allow MAC address changes. This includes e.g. licenses which are bound to certain MAC addresses or redundancy/cluster mechanisms which lead to MAC address changes.

4.2.3.1 Isolation of Management and Production Traffic

It is recommended to isolate the vSphere management traffic from the production traffic by using a separate physical network card bound to a separate vSwitch. If a separate physical network card is not available, it should at least be isolated on the logical layer with VLANs.

4.3 Active Directory Design

4.3.1 Implement a Dedicated Active Directory Forest for EOL Servers

In order to effectively isolate EOL servers and applications, create a dedicated Active Directory forest for EOL servers and applications. The forest will be designated in this concept as *eol.internal*.

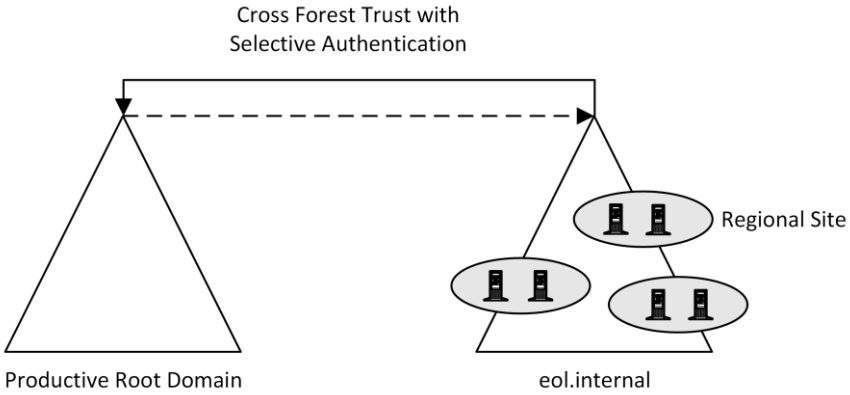

Figure 1 Proposed Active Directory design

Implementation Recommendations

Aspect	Recommendation
Operating system version	Windows Server 2008 R2 with current SP
Domain functional level	Windows Server 2008 R2
Forest functional level	Windows Server 2008 R2
Number of domains within eol.internal	One domain. For operational reasons, not more than one domain should be created. For security reasons, a one-domain forest is sufficient.
Number of Active Directory sites in the forest eol.internal	One Active Directory site per datacentre region is recommended.
Number of Domain Controllers	At least one per Active Directory site.
OU Design	Create a suitable OU design that fits your requirements.
Group Policy design	Create a suitable Group Policy design that fits your requirements. When the OU design is complete, you can create additional OU structures for the application of Group Policies to users and computers and to limit the visibility of objects.

Implementation Guidance

http://technet.microsoft.com/en-us/library/cc772464(v=ws.10).aspx

http://technet.microsoft.com/en-us/library/cc770377(v=ws.10).aspx

http://technet.microsoft.com/de-de/magazine/2008.05.oudesign.aspx

http://technet.microsoft.com/en-us/library/cc754948(v=ws.10).aspx

4.3.2 Implement a Cross Forest Trust between the Forest Root Domain and eol.internal

In order to enable Kerberos-based authentication between the forest root domain and the forest eol.internal, a Cross Forest Trust should be implemented.

Implementation Recommendations

Aspect	Recommendation
Trust directions	If possible: a) One way trust: trusting forest is eol.internal, trusted forest is the productive root domain. b) Authentication requests from eol.internal to the productive root domain should be avoided. If they are however necessary, a two-way cross forest trust should be implemented. If a two-way cross forest will be implemented it should be evaluated, if the two-way direction might be a temporary solution.
SID filter quarantining	If EOL servers are being migrated (instead of a clean installation in the new forest), SIDs should preferably not be migrated. Thus, SID filter quarantining (which is the default configuration for the cross forest trust) should not be disabled.

Implementation Guidance

http://technet.microsoft.com/en-us/library/cc771397.aspx

http://technet.microsoft.com/en-us/library/cc816880(WS.10).aspx

http://technet.microsoft.com/en-us/library/1f33e9a1-c3c5-431c-a5cc-c3c2bd579ff1

http://technet.microsoft.com/en-us/library/cc816580(v=ws.10).aspx

4.3.3 Populate EOL Server Forest with Member Servers and Member Workstations

Aspect	Recommendation
Populate eol.internal with EOL member servers	a) Preferable solution: do a clean EOL server installation in the pristine forest and migrate only applications and application data from the original system to the freshly installed EOL servers. b) Alternative solution to a): remove the EOL server(s) from its original domain and join it to the eol.internal domain.
Member workstations	a) Member workstations should only be workstations

	for administrative purposes (see 5.1). b) If, however, non-administrative member workstations need to be implemented in the eol.internal forest, these workstations should at least have on operating system level of Windows 7.

Implementation Guidance

http://www.cio.cornell.edu/sites/default/files/Cornell-University-Migration-Planning-Final.docx

http://social.technet.microsoft.com/wiki/contents/articles/11996.interforest-migration-with-admt-3-2-part-1.aspx

http://social.technet.microsoft.com/wiki/contents/articles/11996.interforest-migration-with-admt-3-2-part-1.aspx

http://www.msxfaq.de/migration/org2org.htm

5 SECURING ADMINISTRATION OF EOL SERVER ENVIRONMENT

5.1 Implement Secure Administration Hosts

"Secure administrative hosts are workstations or servers that have been configured specifically for the purposes of creating secure platforms from which privileged accounts can perform administrative tasks in Active Directory or on domain controllers, domain-joined systems, and applications running on domain-joined systems. In this case, "privileged accounts" refers not only to accounts that are members of the most privileged groups in Active Directory, but to any accounts that have been delegated rights and permissions that allow administrative tasks to be performed [..]A secure administrative host can be a dedicated workstation that is used only for administrative tasks, a member server that runs the Remote Desktop Gateway server role and to which IT users connect to perform administration of destination hosts, or a server that runs the Hyper-V® role and provides a unique virtual machine for each IT user to use for their administrative tasks. In many environments, combinations of all three approaches may be implemented." (See [ADBP], p. 66)

Sample approaches to implementing secure administrative hosts are the following:

Sample approach	Evaluation
(a) Implementing separate physical workstations "One way that you can implement administrative hosts is to issue each IT user two workstations. One workstation is used with a "regular" user account to perform activities such as checking email and using productivity applications, while the second workstation is dedicated strictly to administrative functions. For the productivity workstation, the IT staff can be given regular user accounts rather than using privileged accounts to log on to unsecured computers. The administrative workstation should be configured with a stringently controlled configuration and the IT staff should use a different account to log on to the administrative workstation." (See [ADBP], p. 71)	**Pros** "By implementing separate physical systems, you can ensure that each computer is configured appropriately for its role and that IT users cannot inadvertently expose administrative systems to risk." (See [ADBP], p. 71) **Cons** ■ "Implementing separate physical computers increases hardware costs. ■ Logging on to a physical computer with credentials that are used to administer remote systems caches the credentials in memory. ■ If administrative workstations are not stored securely, they may be vulnerable to compromise via mechanisms such as physical hardware key loggers or other physical attacks." (See [ADBP], p. 71)
(b) Implementing a secure physical workstation with a virtualized productivity workstation "In this approach, IT users are given a secured administrative workstation from which they can perform day-to-day administrative functions, using Remote Server Administration Tools (RSAT) or RDP connections to servers within their scope of responsibility. When IT users need to perform productivity tasks, they can connect via RDP to a remote productivity workstation running as a virtual machine. Separate credentials should be used for	**Pros** ■ "Administrative workstations and productivity workstations are separated. ■ IT staff using secure workstations to connect to productivity workstations can use separate credentials and smart cards, and privileged credentials are not deposited on the less-secure computer." (See [ADBP], p. 72) **Cons**

each workstation, and controls such as smart cards should be implemented." (See [ADBP], p. 71f)	■ "Implementing the solution requires design and implementation work and robust virtualization options. ■ If the physical workstations are not stored securely, they may be vulnerable to physical attacks that compromise the hardware or the operating system and make them susceptible to communications interception." (See [ADBP], p. 72)
(c) Implementing a single secure workstation with connections to separate "productivity" and "administrative" virtual machines "In this approach, you can issue IT users a single physical workstation that is locked [...], and on which IT users do not have privileged access. You can provide Remote Desktop Services connections to virtual machines hosted on dedicated servers, providing IT staff with one virtual machine that runs email and other productivity applications, and a second virtual machine that is configured as the user's dedicated administrative host." (See [ADBP], p. 72)	**Pros** ■ "IT users can use a single physical workstation. ■ By requiring separate accounts for the virtual hosts and using Remote Desktop Services connections to the virtual machines, IT users' credentials are not cached in memory on the local computer. ■ The physical host can be secured to the same degree as administrative hosts, reducing the likelihood of compromise of the local computer. ■ In cases in which an IT user's productivity virtual machine or their administrative virtual machine may have been compromised, the virtual machine can easily be reset to a "known good" state. ■ If the physical computer is compromised, no privileged credentials will be cached in memory, and the use of smart cards can prevent compromise of credentials by keystroke loggers. **Cons** ■ Implementing the solution requires design and implementation work and robust virtualization options. ■ If the physical workstations are not stored securely, they may be vulnerable to physical attacks that compromise the hardware or the operating system and make them susceptible to communications interception." (See [ADBP], p. 72f)
(d) Implementing jump servers "As an alternative to secure administrative workstations, or in combination with them, you can implement secure jump servers, and administrative users can connect to the jump servers using RDP and smart cards to perform administrative tasks. Jump servers should be configured to run the Remote	**Pros** ■ "Creating jump servers allows you to map specific servers to "zones" (collections of systems with similar configuration, connection, and security requirements) in your network and to require that the administration of each zone is achieved by administrative staff connecting from secure

Desktop Gateway role to allow you to implement restrictions on connections to the jump server and to destination servers that will be managed from it. If possible, you should [...] create Personal Virtual Desktops or other per-user virtual machines for administrative users to use for their tasks on the jump servers. By giving the administrative users per-user virtual machines on the jump server, you provide physical security for the administrative workstations, and administrative users can reset or shut down their virtual machines when not in use. [...] Wherever possible, remote administration tools should be used to manage servers. The Remote Server Administration Tools (RSAT) feature should be installed on the users' virtual machines (or the jump server if you are not implementing per-user virtual machines for administration), and administrative staff should connect via RDP to their virtual machines to perform administrative tasks. In cases when an administrative user must connect via RDP to a destination server to manage it directly, RD Gateway should be configured to allow the connection to be made only if the appropriate user and computer are used to establish the connection to the destination server. Execution of RSAT (or similar) tools should be prohibited on systems that are not designated management systems, such as general-use workstations and member servers that are not jump servers." (See [ADBP], p. 73f).	administrative hosts to a designated "zone" server. ■ By mapping jump servers to zones, you can implement granular controls for connection properties and configuration requirements, and can easily identify attempts to connect from unauthorized systems. ■ By implementing per-administrator virtual machines on jump servers, you enforce shutdown and resetting of the virtual machines to a known clean state when administrative tasks are completed. By enforcing shutdown (or restart) of the virtual machines when administrative tasks are completed, the virtual machines cannot be targeted by attackers, nor are credential theft attacks feasible because memory-cached credentials do not persist beyond a reboot. **Cons** ■ Dedicated servers are required for jump servers, whether physical or virtual. ■ Implementing designated jump servers and administrative workstations requires careful planning and configuration that maps to any security zones configured in the environment." (See [ADBP], p. 74)

Summarized recommendations

Aspect	Recommendation
Implementation of secure administration hosts	a) Evaluate which sample approach for implementing secure administration hosts fits best to the operational requirements. From the authors perspective a combination of the sample approach (b) (a secure physical workstation with a virtualized productivity workstation) and (d) (jump servers) fits best, because the concept of jump servers is already in use. Because it might eventually not be appropriate for all administrative personnel, the approach (b) will complete the secure administration. c) Implement secure administration hosts for the EOL server environment that are different from secure administration hosts for the productive environment.

	d) Implement hardening of the secure administration hosts (see implementation guidance).

Implementation Guidance

[ADBP], p. 65-74 (general guidance)

[ADBP], p. 66-70 (hardening guidance)

[PtHv2], p. 18f

5.2 Implement Privilege Tiers for Administrative Accounts

Implement privilege tiers for administrative accounts as recommended by Microsoft (see [PtHv2], p. 15):

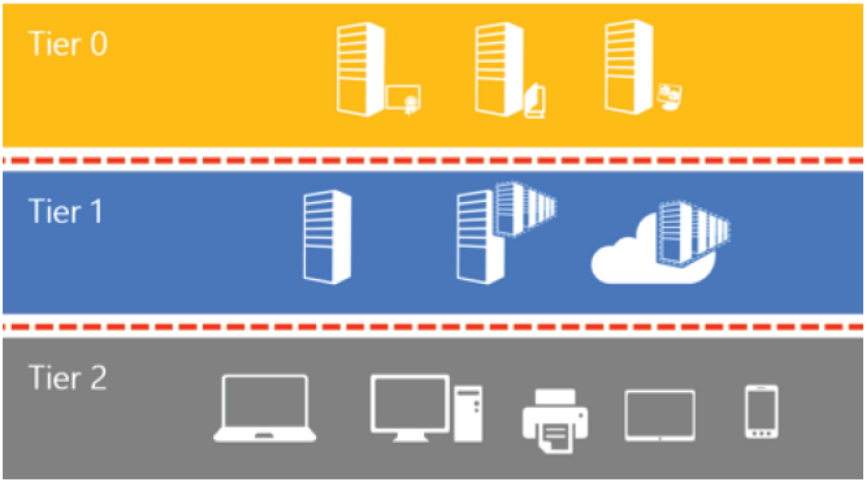

Figure 2 Tier model for administrative accounts

Specific business needs may require other tiers or additional segmentation, but this model can be used as a starting point.

Tier definitions

Tier	Tier description	Membership samples of predefined administrative accounts
Tier 0	"Forest admins: Direct or indirect administrative control of the Active Directory forest, domains, or domain controllers." (See [PtHv2], p. 15.)	Enterprise Admins, built-in Administrators of the domain, Schema Admins, Domain Admins.
Tier 1	"Server admins: Direct or indirect administrative control over a single or multiple servers." (See [PtHv2], p. 15.)	Members of the built-in Administrators group on the server, Server Operators, Backup Operators, Account Operators.
Tier 2	"Workstation Admins: Direct or indirect administrative control over a single or multiple devices." (See [PtHv2], p. 15.)	Members of the built-in Administrators group on the workstation. Ideally, this tier should be empty in eol.internal. If not, there should be a very small number of administrative accounts.

5.3 Implement Secure Administration Principles

Each of the following principles (that are cited from [PtHv2, p.15ff) should be implemented in the eol.internal forest:

- Each administrative resource (group, account, servers, workstation, Active Directory object, or application) has to be classified as belonging to only one tier.
- Personnel with responsibilities at multiple tiers must have separate administrative accounts created for each required tier. Any account that currently logs on to multiple tiers must be split into multiple accounts, each of which fits within only one tier definition. These accounts must also be required to have different passwords.
- Administrative accounts may not control higher-tier resources through administrative access such as access control lists (ACLs), application agents, or control of service accounts. Accounts that control a higher tier may not log on to lower-tier computers because logging on to such a computer may expose and inadvertently grant control of the account credentials and privileges assigned to that account. Under some specific exceptions, a feature that supports Remote Desktop (RDP) with restricted admin mode could be used without exposing credentials.[8]
- Administrative accounts may control lower-tier resources as required by their role, but only through management interfaces that are at the higher tier and that do not expose credentials—for example, domain admin accounts (tier 0) managing server admin Active Directory account objects (tier 1) through Active Directory management consoles on a domain controller (tier 0).

  Figure 3 visually depicts the logon restrictions for the tier model:

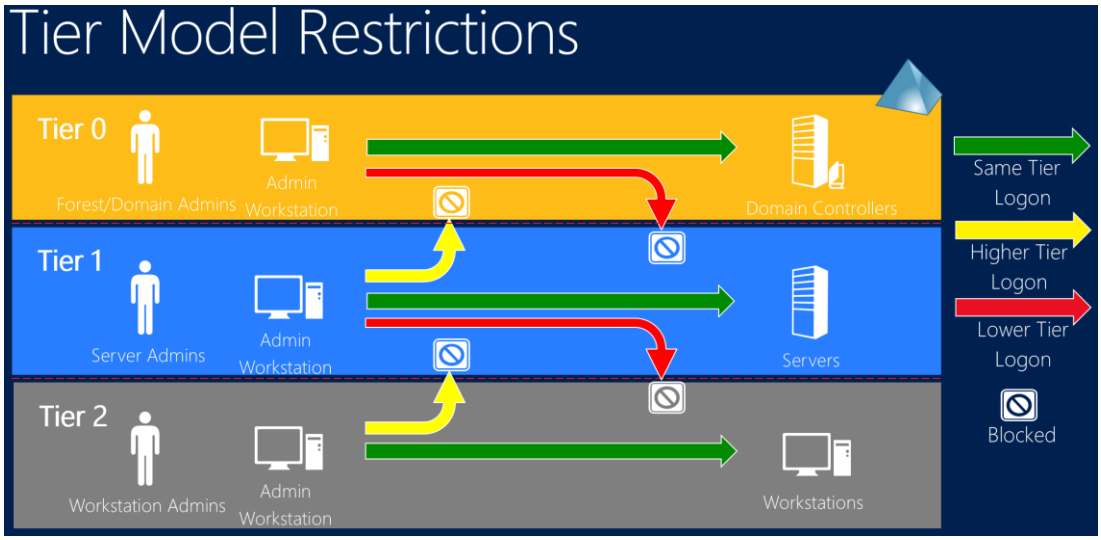

Figure 3 Tier model restrictions

- Limit the number of administrative accounts, especially in tier 0. The schema admin group should have members only on demand.
- Limit the number of hosts on which administrative credentials are exposed.
- Limit role privileges to the minimum required.
- Create a special group with the debug privilege and grant membership to this group only on demand (administrative accounts should not be member of this group by default).
- Enforce logon restrictions to ensure that:
  - Domain admins (tier 0) cannot log on to enterprise servers (tier 1) and standard user workstations (tier 2).
  - Server administrators (tier 1) cannot log on to standard user workstations (tier 2).

[8] *Availability and configuration of restricted admin mode for RDP connections, see [PtHv2], p. 35f.*

Implementation Guidance

[PtHv2], p.17 (how to implement logon restrictions)

[ADBP], p. 45-57

6 Securing Domain Controllers

In order to reduce the attack surface of domain controllers, implement the following controls:

Aspect /Recommendation	Description
Implement physical security for domain controllers	The eol.internal domain controllers should be physically secured such as the productive domain controllers of the root domain forest.
Physical domain controller	At least one domain controller should be a physical domain controller (in case of a damage of the virtual domain controllers).
Virtual domain controller	Implement domain controllers as virtual domain controllers (apart from at least one physical domain controller). "If you implement virtual domain controllers, you should ensure that domain controllers run on separate physical hosts than other virtual machines in the environment." ([ADBP], p. 76) "You should also consider separating the storage of virtual domain controllers to prevent storage administrators from accessing the virtual machine files." ([ADBP], p. 76)
Branch locations	So far, domain controllers of eol.internal will not be located in branch locations. If, however, this becomes necessary, these domain controllers should be installed as Read Only Domain Controllers (RODC).
Implement a secure configuration of domain controllers	**a) "All domain controllers should be locked down upon initial build** This can be achieved using the Security Configuration Wizard that ships natively in Windows Server to configure service, registry, system, and WFAS settings on a "base build" domain controller. Settings can be saved and exported to a GPO that can be linked to the Domain Controllers OU in each domain in the forest to enforce consistent configuration of domain controllers. If your domain contains multiple versions of Windows operating systems, you can configure Windows Management Instrumentation (WMI) filters to apply GPOs only to the domain controllers running the corresponding version of the operating system." ([ADBP], p. 77) But be aware that the security configuration will probably have to be lowered /adapted because of the Windows Server 2003 member servers. This refers exemplarily – but is not limited – to the "LAN manager authentication level" settings. **b) Use Microsoft Security Compliance Manager (SCM) to harden domain controllers** In order to produce a template for security baseline for eol.internal domain controllers use SCM. The template created in SCM can be exported from SCM to a GPO that should be linked to the OU containing the domain controllers of eol.internal. But be aware that the security configuration will probably have to be lowered /adapted because of the Windows Server 2003 member servers. This refers exemplarily – but is not limited – to the "LAN manager authentication level" settings. **c) Implement RDP restrictions** 'Group Policy Objects that link to all domain controllers OUs in the forest should be configured to allow RDP connections only from authorized users and systems — that is, jump servers

	/administrative hosts. This can be achieved through a combination of user rights settings and Windows Firewall with Advance Security (WFAS) configuration and should be implemented in GPOs so that the policy is consistently applied. If it is bypassed, the next Group Policy refresh returns the system to its proper configuration.' (Compare [ADBP], p. 78) **d) Block internet access for domain controllers** "One of the checks that is performed as part of an Active Directory Security Assessment is the use and configuration of Internet Explorer on domain controllers. Internet Explorer (or any other web browser) should not be used on domain controllers, but analysis of thousands of domain controllers has revealed numerous cases in which privileged users used Internet Explorer to browse the organization's intranet or the Internet [...] Launching web browsers on domain controllers should be prohibited not only by policy, but by technical controls, and domain controllers should not be permitted to access the Internet. If your domain controllers need to replicate across sites, you should implement secure connections between the sites. Although detailed configuration instructions are outside the scope of this document, you can implement a number of controls to restrict the ability of domain controllers to be misused or misconfigured and subsequently compromised." ([ADBP], p. 78f) **e) Prevent web browsing from domain controllers** "You can use a combination of AppLocker configuration, "black hole" proxy configuration, and WFAS configuration to prevent domain controllers from accessing the Internet and to prevent the use of web browsers on domain controllers." ([ADBP], p. 79f) **f) Implement the following security controls in order to mitigate Pass-the-Hash attacks** ■ Logon restrictions with new well-known security identifiers (SIDs) ■ Enforce credential removal after logoff ■ Remove LAN Manager (LM) hashes from LSASS ■ Remove plaintext credentials from LSASS for domain accounts ■ Restricted Admin mode for Remote Desktop ■ Protected Users security group **g) Configure domain controller audit policy settings in the Default Domain Controllers OU according to recommendations in section 8.2** **Optional:** **h) Implement AppLocker policy on domain controllers** "AppLocker or a third-party application whitelisting tool should be used to configure services and applications that are permitted to run on domain controllers, and these permitted applications and services should be comprised only of what is required for the computer to host AD DS and possibly DNS, plus any system security software such as antivirus software. By whitelisting permitted applications on domain controllers, an additional layer of security is added so that even if an unauthorized application is installed on a domain controller, the application cannot run." ([ADBP], p. 78)

Implementation Guidance

[ADBP], p. 75-79

[PtHv2], p. 18f, p. 31-42 (for PtH mitigations)

http://technet.microsoft.com/en-us/library/cc771744(WS.10).aspx (RODC implementation guide)

http://technet.microsoft.com/en-us/library/cc677002.aspx (Microsoft Security Compliance Manager)

7 SECURING EOL SERVERS

This section applies to Windows Server 2003 as future (at the time of writing of this concept, Windows Server 2003 is not an EOL operating system) EOL servers. Although each Windows system should be part of an Active Directory (for operational reasons), there might exist reasonable exceptions that require a stand-alone system. The recommended security settings of this section apply to a Windows Server 2003 system whether it is part of an Active Directory or not.

7.1 Securing the Operating System

Technically securing the Windows operating systems might be split into two parts:

- Implementation of security settings that are deployable via GPOs.
- Security settings that cannot be deployed via GPO. These settings are summarized together with security best practices for Windows servers in section 7.1.3.

7.1.1 Implement a Suitable OU Design

Aspect	Recommendation
In order to utilize security settings that are deployable via GPO in an efficient manner, a well-structured OU design is required.	a) Create a Member Server OU in the eol.internal forest. The Member Server Baseline Policy (MSBP) will be linked to that OU. b) Create a subordinated OU for every Windows Server 2003-based server role. The server role specific GPO will be linked to that OU. c) Populate OUs with member servers according to their member server role. d) For stand-alone servers, steps a) to c) are not required. The MSBP and subsequent GPOs will be applied only locally.

Implementation Guidance

[S03Sec], p. 24 (for the recommended OU design) or section 10.1

7.1.2 Implement a Baseline Security GPO Template for EOL Servers

In 2006, Microsoft published a comprehensive security guide for Windows Server 2003 [S03Sec]. This security guide is still the benchmark for Windows Server 2003-based security. The majority of the recommended security settings are from this guide.

Aspect	Recommendation
[S03Sec] offers three types of templates for the baseline security level and for each server role according to the desired security level. The three levels are: ■ "Legacy Client (LC)": low security level for compatibility with Windows 2000 and Windows NT 4.0.	a) Create a Member Server Baseline Policy (MSBP) with the EC level and link this OU to the Member Server OU. b) For reasons of simplicity, use a minimum of server roles.

■ "Enterprise Client (EC)": appropriate security level for Windows Server 2003 systems in enterprise environments. ■ "Specialized Security – Limited Functionality (SSLF)": "This environment provides much stronger security than the EC environment [...]In the SSLF environment, security concerns are so great that significant loss of client functionality and manageability is considered an acceptable trade-off if the highest levels of security can be achieved." ([S03Sec], 50) The GPO-files with the security settings are included in [S03Sec].	c) Create an EC-level GPO for each server role and link this GPO to the subordinated OU for every Windows Server 2003-based server role. d) For stand-alone servers, steps a) and c) are not required. The MSBP and subsequent GPOs will be applied only locally. Optional: e) Evaluate and implement the SSLF security level as MSBP and server role GPO.

Implementation Guidance

[S03Sec], p. 49-118 (for MSBP).

For additional information concerning logging und monitoring, with reference to (Windows Server 2008 R2-based) domain controllers and (Windows 7-based) administrative clients, see section 8).

7.1.3 Security Best Practices for Windows Servers

Aspect	Recommendation
1. Password policy	"In many operating systems, the most common method to authenticate a user's identity is to use a secret passphrase or password. A secure network environment requires all users to use strong passwords, which have at least eight characters and include a combination of letters, numbers, and symbols. These passwords help prevent the compromise of user accounts and administrative accounts by unauthorized users who use manual methods or automated tools to guess weak passwords. Strong passwords that are changed regularly reduce the likelihood of a successful password attack." [PwdPol] To ensure the usage of secure passwords, a well-defined password policy should be utilized and enforced through Group Policy settings.
2. Data Execution Prevention (DEP)	Implement data execution prevention (DEP) "Data execution prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits." [DEP] DEP should be set for all processes (OptOut). In OptOut mode administrators can manually create a list of

	specific applications that do not have DEP enabled. These settings should be managed centrally, for example through: ■ Startup Scripts [StUp] or ■ ADM/ADMX Files [AdminTemp].
3. Additional NTFS permissions	Implement additional NTFS permissions For certain security relevant files, additional NTFS permissions should be implemented as stated in [S03Sec], p. 109. It is recommended to use/implement the "Optional-File-Permissions.inf", which is included with the downloadable version of the guide. Executables that run with high privileges should have set appropriate NTFS permissions. NTFS permissions should always be set, so that access to high privilege objects is only allowed for high privilege users. For example, standard user should not have write permissions for services which are running under the "SYSTEM" account.
4. Restricted groups	Implement restricted groups for privileged local accounts "The Backup Operators and Power Users groups are restricted in all three environments that are defined in this guide. Although members of the Backup Operators and Power Users groups have less access than members in the Administrators group, they still have powerful capabilities [...]Administrators should configure restricted groups by adding the desired group directly to the MSBP. When a group is restricted, you can define its members and any other groups to which it belongs. If you do not specify these group members, the group remains totally restricted." ([S03Sec], p. 108) Additionally the following groups should be defined as restricted: Administrators, Server Operators.
5. Debug privilege	Implement a dedicated security group with enabled debug privilege The debug privilege allows the debugging of processes that are otherwise not accessible. For example, a process running as a user with the debug privilege enabled can debug a service running as local system. This enables an attacker to use hacking tools, such as "mimikatz" to access clear text passwords of logged on users or other credential data. As the debug privilege is active by default for all

	administrators through the MSBP, a separate GPO has to be defined, disabling the debug privilege for all users not needing it. The process order of Group Policy settings has to be considered[9].
6. EMET	Implement EMET on EOL servers "The Enhanced Mitigation Experience Toolkit (EMET) is a utility that helps prevent vulnerabilities in software from being successfully exploited. EMET achieves this goal by using security mitigation technologies. These technologies function as special protections and obstacles that an exploit author must defeat to exploit software vulnerabilities." [EMET] EMET supports the central management of settings via ADMX files. Therefore settings should always be managed centrally.

Implementation Guidance

[DEP] *http://support.microsoft.com/kb/875352*

[StUp] *http://technet.microsoft.com/en-us/library/cc779329(v=ws.10).aspx*

[AdminTemp] *http://technet.microsoft.com/en-us/magazine/2008.01.layout.aspx*

[EMET] *http://support.microsoft.com/kb/2458544/en*

[S03Sec], p. 108 (for restricted groups)

http://msdn.microsoft.com/en-us/library/aa291232(v=vs.71).aspx (for debug privilege)

http://technet.microsoft.com/en-us/library/hh994572(v=ws.10).aspx (for password policy)

[9] *See http://technet.microsoft.com/en-us/library/cc785665(v=ws.10).aspx*

7.2 Securing 3rd Party Applications

This concept provides some general information about 3rd Party application hardening.

Aspect	Recommendation
1. Service Accounts	Implement Service Accounts according to the following principles: • Least privilege principle (avoid Local System account; use Local Service and Network Service accounts if applicable). • Creation of strong passwords with 12 or more characters and complexity requirements[10] must be met. • Critical accounts with high-level privileges should not accept unauthorized commands over the network. This has to be checked accordingly.
2. 3rd party patch management	Implement a patch and vulnerability management process for: ■ Third-party applications running on EOL systems. ■ All installed third-party software components, such as, and especially, out-dated Java versions. Timely patching of security issues ensures operational availability, confidentiality, and integrity of the EOL server systems.
3. Security logging on application level	Implement base security logging on the application level In case the application running on the EOL server system allows for the logging of security relevant events, this should be done and the results should be monitored evaluated respectively.
4. Application hardening	If operationally feasible, implement application specific hardening In addition to the hardening of the operating system, specific security configuration options for the hardening of applications running on the EOL server systems, should be evaluated and when ever possible implemented. This reduces the attack surface of the entire system.

Implementation Guidance

http://technet.microsoft.com/en-us/library/cc875826.aspx (for Service Accounts)

[10] *See http://technet.microsoft.com/en-us/library/cc786468(v=ws.10).aspx,*

8 MONITORING AND LOGGING

A solid event log monitoring system is a crucial part of any secure design. Many computer security compromises could be discovered early in the event if the victims enacted appropriate event log monitoring and alerting. Independent reports have supported this insight.

8.1 Collect Computer Events Centrally

"Multiple options exist for centralized event log collection and management, [...] Third-party solutions such as security information and event management (SIEM) solutions may provide agents for collection and alerting for specific events. [...] Log collections should be enabled for as many computers as possible and configured to push the events from these computers quickly."([PtHv2], p.24) See also chapter 7.2.

8.2 Implement a Windows Audit Policy

<table>
<tr><th>Aspect /Recommendation</th><th>Description</th></tr>
<tr><td>Implement an Audit Policy

"Each audit policy category can be enabled for Success, Failure, or Success and Failure events." ([ADBP], p. 81-82)

The recommended domain controller settings are to be configured in the Default Domain Controllers GPO (see section 6 (g)) and are based on the recommendations of [ADBP], p. 99-109.

The recommended Windows Server 2003 settings are configured in the MSBP GPO (see section 7.1.2).</td><td>
<table>
<tr><th>Audit Policy Category</th><th>Description</th><th>Recommended Setting</th></tr>
<tr><td>1. Audit account logon events</td><td>"Reports each instance of a security principal (for example, user, computer, or service account) that is logging on to or logging off from one computer in which another computer is used to validate the account. Account logon events are generated when a domain security principal account is authenticated on a domain controller."([ADBP], p. 82)</td><td>Domain Controller:
Enabled: Success and Failure
Member Server:
Enabled: Success and Failure
Admin Client:
Enabled: Success and Failure</td></tr>
<tr><td>2. Audit account management</td><td>"This audit setting determines whether to track management of users and groups. For example, users and groups should be tracked when a user or computer account, a security group, or a distribution group is created, changed, or deleted; [...]"([ADBP], p. 82)</td><td>Domain Controller:
Enabled: Success
Member Server:
Enabled: Success
Admin Client:
Enabled: Success</td></tr>
<tr><td>3. Audit directory service access</td><td>"This policy setting determines whether to audit security principal access to an Active Directory object that has its own specified system access control list (SACL)." ([ADBP], p. 82)</td><td>Domain Controller: No Auditing
Member Server:
No Auditing</td></tr>
</table>
</td></tr>
</table>

Aspect /Recommendation	Description		
The recommended Admin Client settings are based on the recommendations of *http://technet.microsoft.com/en-us/library/dn487457.aspx*.			**Admin Client:** No Auditing
	4. Audit logon events	"Logon events are generated when a local security principal is authenticated on a local computer. Logon Events records domain logons that occur on the local computer [...]." ([ADBP], p. 82)	**Domain Controller:** Enabled: Success and Failure **Member Server:** Enabled: Success and Failure **Admin Client:** Enabled: Success and Failure
	5. Audit object access	"Object Access can generate events when subsequently defined objects with auditing enabled are accessed (for example, Opened, Read, Renamed, Deleted, or Closed). [...] This category is very "noisy" and will generate five to ten events for each object access. [...] It should only be enabled when needed." ([ADBP], p. 83)	**Domain Controller:** No Auditing **Member Server:** No Auditing **Admin Client:** No Auditing
	6. Audit policy change	"This policy setting determines whether to audit every incidence of a change to user rights assignment policies, Windows Firewall policies, Trust policies, or changes to the audit policy. [...]"([ADBP], p. 83)	**Domain Controller:** Enabled: Success and Failure **Member Server:** Enabled: Success **Admin Client:** Enabled: Success and Failure
	7. Audit privilege use	"There are dozens of user rights and permissions in Windows (for example, Logon as a Batch Job and Act as Part of the Operating System). This policy setting determines whether to audit each instance of a security principal by exercising a user right or privilege. [...]"([ADBP], p. 83)	**Domain Controller:** No Auditing **Member Server:** No Auditing **Admin Client:** No Auditing
	8. Audit process tracking	"This policy setting determines whether to audit detailed process tracking information for events such as program activation, process exit,	**Domain Controller:**

Aspect /Recommendation	Description		
		handle duplication, and indirect object access. [...]" ([ADBP], p. 83)	Enabled: Success **Member Server:** No Auditing **Admin Client:** Enabled: Success
	9. Audit system events	"System Events is almost a generic catch-all category, registering various events that impact the computer, its system security, or the security log. It includes events for computer shutdowns and restarts, power failures, system time changes, authentication package initializations, audit log clearings, impersonation issues, and a host of other general events. [...]"([ADBP], p. 83)	**Domain Controller:** Enabled: Success and Failure **Member Server:** Enabled: Success and Failure **Admin Client:** Enabled: Success and Failure

Implementation Guidance

[ADBP], p. 81-96

[S03Sec], p. 52-64

http://technet.microsoft.com/en-us/library/dn487457.aspx

8.3 Respond to Suspicious Activity

"A key element of a comprehensive security strategy is the ability to respond to suspicious activity and ensure that the right resources are rapidly engaged to evaluate, prioritize, investigate, and act on events. Some alerts may warrant immediate response, while others may be prioritized at a lower level to ensure that resources are reserved for the most important events. Microsoft recommends integrating the following elements in an incident response process:

- Regularly update protection and detection mechanisms to limit false positive alerts from reoccurring.
- After each significant security event or compromise, update protection and detection mechanisms to prevent future attacks from reoccurring.
- After a compromise, continue with close observation of affected hosts and accounts to ensure that the attacker is not able to regain access.

Aspect /Recommendation	Description
Implement an Advanced Audit Policy	"Starting with Windows Vista and Windows Server 2008, Microsoft improved the way event log category selections can be made by creating subcategories under each main audit category. Subcategories allow auditing to be far more granular than it could otherwise by using the main categories. By using subcategories, you can enable only portions of a particular main category, and skip generating events for which you have no use. Each audit policy subcategory can be enabled for Success, Failure, or Success and Failure events." ([ADBP], p. 84) Based on the incident, the administrators must individually define which objects will have auditing enabled.

- If a compromise has occurred, proceed to recovery plans and ensure that attack vectors are properly addressed. Consider delaying recovery efforts to track attacker behaviour and uncover the intent or attack details. This information could lead to a better recovery strategy." ([PtHv2], p.24)

Implementation Guidance

[PtHv2], p.24

[ADBP], p. 84

9 Adaptation of Processes for Secure Operations

Processes for secure operation of the IT infrastructure already implemented may be adapted to the new EOL server (and application) environment.

Processes for secure operation are:

- Asset Management
- Risk Assessment for applications running on EOL servers
- Patch & Vulnerability Management (for EOL servers and applications running on EOL servers)
- Change Management
- Incident Response Management
- Disaster Recovery and Business Continuity Management

The enterprise should evaluate if these processes for the EOL environment are to be integrated in the hitherto existing teams or if the EOL environment requires a dedicated team for these processes. However, dedicated EOL server and application know-how will be needed.

10 APPENDIX

10.1 Recommended OU Structure & Design

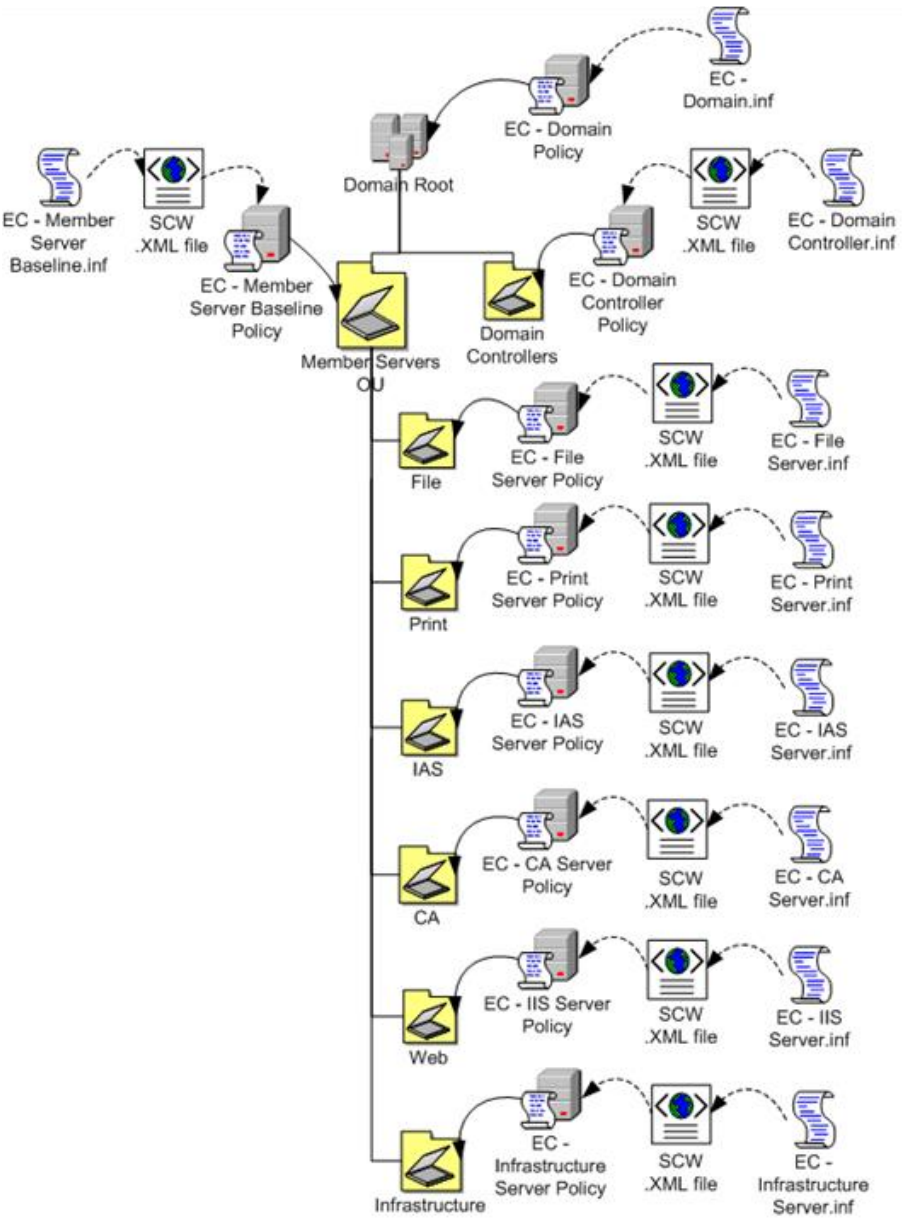

Figure 4 Recommended OU design

(See [S03Sec], p. 24).

10.2 References

[ERNW_Pentest] Enno Rey, Michael Thumann, Dominick Baier : Mehr IT-Sicherheit durch Pen-Tests, Vieweg Verlag Wiesbaden, 2005.

[ADBP] Microsoft IT / Information Security and Risk Management: Best Practices for Securing Active Directory, Published: April 2013 (*http://aka.ms/bpsad*)

[PtHv1] Microsoft Trustworthy Computing (TwC): Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques. Mitigating the risk of lateral movement and privilege escalation, 2012 (*http://www.microsoft.com/en-gb/download/details.aspx?id=36036*)

[PtHv2] Microsoft Trustworthy Computing (TwC): Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques, Version 2, 07.07.2012 (*http://www.microsoft.com/en-gb/download/details.aspx?id=36036*)

[S03Sec] Microsoft Corporation: Microsoft Solutions for Security and Compliance. Windows Server 2003 Security Guide, 2006, *http://www.microsoft.com/en-us/download/details.aspx?id=8222*

[PwdPol] Microsoft Technet: Password Policy (http://technet.microsoft.com/en-us/library/hh994572(v=ws.10).aspx)

10.3 Disclaimer