Microsoft Windows

Common Criteria Evaluation

Microsoft Windows Server 2008 Hyper-V

Evaluated Configuration Guide

Document Information	
Version Number	1.9
Updated On	Monday, June 29, 2009

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

Microsoft, Active Directory, Visual Basic, Visual Studio, Windows, the Windows logo, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

1 Overview

Welcome to the *Hyper-V Common Criteria Guide*. This guide describes how to setup the Hyper-V server role on Windows Server 2008 to meet the same security conditions used by the Common Criteria (CC) evaluation.

Microsoft engineering teams, consultants, support engineers, partners, and customers have reviewed and approved this prescriptive guidance to make it:

- **Proven**. Based on field experience.
- **Authoritative**. Offers the best advice available.
- **Accurate**. Technically validated and tested.
- **Actionable**. Provides the steps to success.
- **Relevant**. Addresses real-world security concerns.

This guide is a supplement to the Hyper-V™ Security Guide, Windows Server 2008 Security Guide, and Windows Server 2003 Security Guide published by Microsoft. It provides the additional installation, configuration, and security information required to reproduce the security level of a Common Criteria-evaluated system.

> **Important** If configuration recommendations in the general technical documentation or Hyper-V, Windows Server 2008, and Windows Server 2003 are not consistent with the instructions in the Hyper-V Evaluation Configuration Guide, the information in the Hyper-V Evaluation Configuration Guide takes precedence and applies.

1.1 Who Should Read This Guide

The *Hyper-V Evaluation Configuration Guide* is primarily for IT professionals, security specialists, network architects, computer engineers, and other IT consultants who plan application or infrastructure development and deployments of Windows Server 2008 for servers in an enterprise environment. The guide is not intended for home users. This guide is for individuals whose jobs may include one or more of the following roles:

- **Security specialist**. Users in this role focus on how to provide security across computing platforms within an organization. Security specialists require a reliable reference guide that addresses the security needs of all segments of their organizations and also offers proven methods to implement security countermeasures. Security specialists identify security features and settings, and then provide recommendations on how their customers can most effectively use them in high risk environments.
- **IT operations, help desk, and deployment staff**. Users in IT operations focus on integrating security and controlling change in the deployment process, and deployment staff focuses on

administering security updates quickly. Staff in these roles also troubleshoot security issues related to applications that involve how to install, configure, and improve the usability and manageability of software. They monitor these types of issues to define measurable security improvements with minimal impact on critical business applications.

- **Network architect and planner**. Users in this role drive the network architecture efforts for computers in their organizations.
- **Consultant**. Users in this role are aware of security scenarios that span all the business levels of an organization. IT consultants from both Microsoft Services and partners take advantage of knowledge transfer tools for enterprise customers and partners.

1.1.1 Skills and Readiness

The following knowledge and skills are required for consultants, operations, help desk and deployment staff, and security specialists who develop, deploy, and secure server systems running Windows Server 2008 in an enterprise organization:

- MCSE on Microsoft Windows Server 2003 or a later certification and two or more years of security-related experience, or equivalent knowledge.
- Experience using Hyper-V Manager.
- Experience in the administration of Windows machines using command line management utilities and scripts.
- Experience in the administration of local users, groups, and policies using command line management utilities.
- Experience configuring Windows Management Instrumentation (WMI) for remote administration.
- Experience using WMI management tools for remote administration including Microsoft Management Console (MMC), eventvwr, and virtmgmt.
- Experience using the Security Configuration Wizard (SCW).
- Experience deploying applications and server computers in enterprise environments.
- In-depth knowledge of the organization's domain and Active Directory environments (OPTIONAL).
- Experience with the Group Policy Management Console and the administration of Group Policy using it (OPTIONAL).

1.2 Section Summaries

This release of the *Hyper-V Evaluation Configuration Guide* consists of this Overview and four sections that discuss how to setup your Hyper-V server role environment to match the security conditions of the evaluated configuration.

1.2.1 Overview

The overview states the purpose and scope of the guide, defines the guide audience, and indicates the organization of the guide to assist you in locating the information relevant to you. It also describes the user prerequisites for the guidance. Brief descriptions follow for each chapter.

1.2.2 Section 1: Introduction

This chapter introduces the Common Criteria standard, specifies further what this guide describes, and provides an implementation roadmap.

1.2.3 Section 2: Specifications and References for a CC-evaluated System

This chapter provides specifications and references for implementing a CC-evaluated Hyper-V server role with Windows Server 2008.

1.2.4 Section 3: Security Policy Assumptions and Conditions

A CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 makes specific assumptions about the required security policy and installation restrictions. Assumptions are items and issues that cannot be formally evaluated under CC but are required to ensure the security level of a CC-evaluated system. Therefore, to reproduce the CC-evaluated implementation of the -V server role of Windows Server 2008, you must review and apply the items in this chapter.

1.2.5 Section 4: Configuring Elevated Security Functionality

A CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 makes specific assumptions about the security functionality included in the evaluation. To install and configure a CC-evaluated implementation of the Hyper-V server role of Windows Server 2008, you must first use the standard technical documentation and guidance for the product. Then you must review and apply the items in this chapter.

1.3 Style Conventions

This guidance uses the style conventions that are described in the following table.

Element	Meaning
Bold font	Signifies characters typed exactly as shown, including commands, switches, and file names. User interface elements also appear in bold.
Italic font	Titles of books and other substantial publications appear in italic.
<Italic>	Placeholders set in italic and angle brackets <Italic> represent variables.

Monospace font	Defines code and script samples.
Note	Alerts the reader to supplementary information.
Important	Alerts the reader to essential supplementary information.

1.4 More Information

The following resources provide additional information about security topics and in-depth discussion of the concepts and security prescriptions in this guide on Microsoft.com:

- Microsoft Hyper-V Server 2008 Configuration Guide - http://www.microsoft.com/downloads/details.aspx?FamilyId=E1E111C9-FA69-4B4D-8963-1DD87804C04F&displaylang=en
- Hyper-V™ Security Guide - http://technet.microsoft.com/en-us/library/dd569113.aspx
- Windows Server 2008 Security Guide - http://go.microsoft.com/fwlink/?LinkId=92552
- Windows Server 2003 Security Guide - http://go.microsoft.com/fwlink/?LinkId=14846
- Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP - http://go.microsoft.com/fwlink/?LinkId=111329
- GPOAccelerator tool and guidance - http://go.microsoft.com/fwlink/?LinkId=107264
- Infrastructure Planning and Design guides - http://go.microsoft.com/fwlink/?LinkId=100915
- Microsoft Assessment and Planning Toolkit - http://go.microsoft.com/fwlink/?LinkId=105520
- Microsoft Deployment page on Microsoft TechNet - http://go.microsoft.com/fwlink/?LinkId=102093
- Microsoft Assessment and Planning Toolkit - http://go.microsoft.com/fwlink/?LinkId=74708
- Microsoft Windows Security Resource Kit - http://go.microsoft.com/fwlink/?LinkId=29168
- Security Guidance page on Microsoft TechNet - http://go.microsoft.com/fwlink/?LinkId=67571
- Solution Accelerators page on Microsoft TechNet - http://go.microsoft.com/fwlink/?LinkId=108308
- HVRemote Documentation, v.05. - HVRemote Documentation 0.5-1.pdf - send e-mail to wincc@microsoft.com to request a digitally signed copy of this guide.

1.5 Support and Feedback

The Solution Accelerators – Security and Compliance (SASC) team would appreciate your thoughts about this and other Solution Accelerators. Please contribute comments and feedback to secwish@microsoft.com. We look forward to hearing from you.

Solution Accelerators provide prescriptive guidance and automation for cross-product integration. They present proven tools and content to help you plan, build, deploy, and operate information technology with confidence. To view the extensive range of Solution Accelerators and for additional information, visit the Solution Accelerators page on Microsoft TechNet (http://go.microsoft.com/fwlink/?LinkId=108308).

2 Introduction

This section focuses on how to setup a Hyper-V server role in Windows Server 2008 to match the security conditions used by the CC evaluation. This guidance is supplemental to the standard technical documentation and security guidance for the product and provides the additional installation, configuration, and security information required to reproduce the security assurance level of an evaluated system. As it is pointed out in Section 1, the guidance in this document has precedence over guidance in any other document in case of discrepancies. See also Section 2.4 for further clarification of the precedence rule.

This section covers the following topics:

- What is Common Criteria?
- What is a CC-compliant System?
- What This Guide Describes
- Implementation Roadmap

2.1 What is Common Criteria?

The Common Criteria for Information Technology (IT) Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO / IEC 15408) for IT security certification. CC provides a general model for evaluation based on constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. Common Criteria is used by governments and organizations around the world to assess the security assurance provided by IT products.

The Common Criteria provides a standardized methodology aimed at establishing the level of confidence that may be placed in the product's security features through expressing security requirements and defining rigorous criteria by which products are evaluated. A product that passes a Common Criteria evaluation receives officially recognized certification. Common Criteria certifications are widely recognized among IT professionals, organizations, government agencies, and customers as a

seal-of-approval for mission-critical software. Note, however, that if a product is CC-certified, it does not necessarily mean it is completely secure. The process of obtaining a CC certification restricts the security analysis to certain security features taken in the context of specific assumptions about the operating environment and the strength of threats faced by the product in that environment. It is intended to provide a level of assurance about the security functions that have been examined by a neutral third party. The CC evaluation also provides help in deciding if the intended use of the system fits the described capabilities.

Common Criteria evaluations can take place in any certificate issuing member country participating in the Common Criteria Mutual Recognition Arrangement (CCMRA). The issued certificates are then accepted globally.

You can find more information about CC at the following Web site:
http://www.commoncriteriaportal.org.

2.2 What is a CC-compliant System?

A system can be considered to be "CC-compliant" if it matches an evaluated and certified configuration. This implies various requirements concerning hardware and software, as well as requirements concerning the operating environment, users, and the ongoing operating procedures.

The hardware and software must match the evaluated configuration. In the case of an operating system, this also requires that the installed kernel, system, and application software are exactly the same as the ones covered by the evaluation. The documentation (including this guide) will specify permitted variations, such as modifying certain configuration files and settings, and installing software that does not have the capability to affect the security of the system (typically those that do not require elevated privileges). Please refer to Section 4.2 of this guide for more information.

Stated requirements concerning the operating environment must also be met. Typical requirements include a secure location for the hardware (protected from physical access by unauthorized persons), level of training of the authorized personnel, as well as restrictions concerning permitted network connections.

The operation of the system must be in agreement with defined organizational security policies, to ensure that actions by administrators and users do not undermine the system's security.

2.3 What This Guide Describes

This guide makes a distinction between two types of Hyper-V utilizations:

- A utilization that serves a general-purpose production environment;
- A utilization that meets the conditions established for the Common Criteria evaluation of this product (cf. Section 2.2). The system configuration that meets these conditions is referred to as a CC-evaluated system in this guide.

A CC-evaluated utilization of Hyper-V makes specific assumptions about installation, configuration, and security. This distinguishes it from most production usages of the product. A CC-evaluated version of the product includes certain restrictions on the way product components are employed and draws specific boundaries around functionality and performance. The purpose of this guide is to describe the assumptions, conditions, and boundaries required to reproduce the configuration and utilization of Hyper-V established in the Common Criteria evaluation.

2.4 Configuration Roadmap

This Common Criteria evaluation is based on the English version of Server Core 2008 and the Hyper-V Server Role and its documentation. You must use only the English-version and refer only to the English-version technical documentation when implementing the CC-evaluated version of Hyper-V. To install and configure a CC-evaluated implementation of Hyper-V, you must first use the standard version 1.0 technical documentation for Hyper-V. Then apply all relevant hardening measures defined in the Security guidance documentation for Server Core 2008 and Hyper-V listed in Section 1.4. Next, refer to the Hyper-V Evaluation Configuration Guide (this document) for supplemental information specific to the Common Criteria requirements. If configuration recommendations in the technical documentation are not consistent with the instructions in the Hyper-V Common Criteria Guide, the information in the Hyper-V Common Criteria Guide takes precedence and applies. For example, if a procedure is described as optional in the Microsoft Hyper-V Server 2008 Configuration Guide (http://www.microsoft.com/downloads/details.aspx?FamilyId=E1E111C9-FA69-4B4D-8963-

1DD87804C04F&displaylang=en) but is required in the Hyper-V Evaluation Configuration Guide, that procedure is required to meet the specifications for Common Criteria compliance.

Use the following checklist as a roadmap to configuring a CC-evaluated version of Hyper-V:

1. Understand the definition and purpose of the Common Criteria standard provided in Sections 2.1 and 2.2.
2. Review the CC-evaluated product specifications, documentation references, and summary of evaluated security functionality in Section 3.
3. Review and apply the policy conditions required for a CC-evaluated system provided in Section 4.
4. Install and configure the Hyper-V Server Role of Server Core 2008 according to the standard installation documentation Microsoft Hyper-V Server 2008 Configuration Guide (http://www.microsoft.com/downloads/details.aspx?FamilyId=E1E111C9-FA69-4B4D-8963-1DD87804C04F&displaylang=en)
5. Harden the Server Core 2008 installation according to Windows Server 2008 Security Guide (http://go.microsoft.com/fwlink/?LinkId=92552)
6. Harden the Hyper-V Server role according to Hyper-V™ Security Guide (http://technet.microsoft.com/en-us/library/dd569113.aspx)
7. Review and apply the security configuration required for a CC-evaluated system according to this guide.

3 Specification and References for a CC-evaluated System

This section provides specifications and references for implementing a Common Criteria (CC)-evaluated Hyper-V server role with Windows Server 2008. It covers the following topics

- About the Evaluated Version of the Hyper-V Server Role of Windows Server 2008
- How to Obtain the CC-Evaluated Product
- Component Specifications for the CC-Evaluated System
- Technical Documentation Guidance and References
- Evaluated and Non-Evaluated Security Functionality

3.1 About the Evaluated Version of the Hyper-V Server Role of Windows Server 2008

The Hyper-V server role of Windows Server 2008 contains security technology that meets the requirements of the Common Criteria Evaluation Assurance Level (EAL) 4+. The system configuration that meets these requirements is referred to as the CC-evaluated system in this guide. The complete list of Hyper-V components is provided in the Hyper-V Attack Surface Reference Workbook (http://download.microsoft.com/download/8/2/9/829bee7b-821b-4c4c-8297-13762aa5c3e4/Windows%20Server%202008%20Hyper-V%20Attack%20Surface%20Reference.xlsx). Please refer to Section 5.1.1.2 for details on how to setup the Hyper-V server role on Windows Server 2008 Core.

The CC evaluation of the Hyper-V server role of Windows Server 2008 was performed on the specific configuration defined in this guide. Note that this covers the use of additional hardware device drivers. Any deviation from this configuration may result in a non-evaluated system, but does not necessarily mean that the security of the resulting system is reduced. It is the responsibility of the individual organization to determine the potential risks and benefits associated with installing newer product versions or additional software that was not subject to this evaluation, and correspondingly deviating from the evaluated configuration described in this document.

The Target of Evaluation (TOE) for this evaluation of Hyper-V is defined as follows:

Product:	*Microsoft Hyper-V Server 2008*
Language:	*English*
Version:	*6.0.6001 Service Pack 1 Build 6001*
Hotfixes installed:	*KB950050 (Hyper-V Update for Windows Server 2008 x64 Edition)*
Underlying processors:	*Hardware-assisted virtualization. This is available in processors that include a virtualization option; specifically, Intel VT or AMD Virtualization (AMD-V) – see Hyper-V Installation Prerequisites (http://technet.microsoft.com/en-us/library/cc731898.aspx) for further details.*

3.1.1 Detailed Hardware Requirements and Supported Guest Operating Systems

3.1.1.1 Memory

The maximum amount of memory that can be used is determined by the type of operating system, as follows:

- For Windows Server 2008 Enterprise and Windows Server 2008 Datacenter, the physical computer can be configured with up to 1 TB of physical memory, and partitions that run either of those editions can be configured with up to 64 GB of memory per partition.

- For Windows Server 2008 Standard, the physical computer can be configured with up to 32 GB of physical memory, and partitions that run either of those editions can be configured with up to 31 GB of memory per partition.

3.1.1.2 Logical CPUs

Hyper-V is supported on physical computers with up to 16 logical processors. A logical processor can be a core processor or a processor using hyper-threading technology. One can configure up to 4 virtual processors on a partition. However, the number of processors supported by a guest operating system might be lower.

The following are some examples of supported systems and the number of logical processors they provide:

- A single-processor/dual-core system provides 2 logical processors.
- A single-processor/quad-core system provides 4 logical processors.
- A dual-processor/dual-core system provides 4 logical processors.
- A dual-processor/quad-core system provides 8 logical processors.
- A quad-processor/dual-core system provides 8 logical processors.
- A quad-processor/dual-core, hyper-threaded system provides 16 logical processors.
- A quad-processor/quad-core system provides 16 logical processors.

3.1.2 Networking

The following networking Hyper-V configurations are supported:

- Each partition can be configured with up to 12 virtual network adapters — 8 can be the "network adapter" type and 4 can be the "legacy network adapter" type. The network adapter type provides better performance and requires a dedicated driver that is included in the integration services packages.
- Each virtual network adapter can be configured with either a static or dynamic MAC address.
- Each virtual network adapter offers integrated virtual local area network (VLAN) support and can be assigned a unique VLAN channel.
- Unlimited number of virtual networks with an unlimited number of partitions per virtual network is also supported.

Important Hyper-V cannot connect a virtual network to a wireless network adapter. As a result, wireless networking capabilities can not be provided to partitions.

3.1.2.1 Storage

The following list of supported Hyper-V physical storage options is supported:

- Direct-attached storage: Serial Advanced Technology Attachment (SATA), external Serial Advanced Technology Attachment (eSATA), Parallel Advanced Technology Attachment (PATA), Serial Attached SCSI (SAS), SCSI, USB, and Firewire.
- Storage area networks (SANs): Internet SCSI (iSCSI), Fibre Channel, and SAS technologies can be used.
- Network-attached storage

The following partition configurations are supported with the following types of virtual storage.

- Virtual hard disks of up to 2040 GB. Hyper-V can use fixed virtual hard disks, dynamically expanding virtual hard disks, and differencing disks.
- Virtual IDE devices. Each partition supports up to 4 IDE devices. The startup disk (sometimes referred to as the boot disk) must be attached to one of the IDE devices. The startup disk can be either a virtual hard disk or a physical disk.
- Virtual SCSI devices. Each partition supports up to 4 virtual SCSI controllers, and each controller supports up to 64 disks. This means that each partition can be configured with as many as 256 virtual SCSI disks.
- Physical disks. Physical disks attached directly to a partition (sometimes referred to as pass-through disks) have no size limitation other than what is supported by the guest operating system.
- Partition storage capacity. Using virtual hard disks, each partition supports up to 512 TB of storage. Using physical disks, this number is even greater depending on what is supported by the guest operating system.
- Partition snapshots. Hyper-V supports up to 50 snapshots per partition.

3.1.2.2 Peripheral Hardware Components

The following peripheral (physical and virtual) hardware components that can be used with Hyper-V:

- DVD Drive
    - A partition has 1 virtual DVD drive by default when you create the partition. Partitions can be configured with up to 3 DVD drives, connected to an IDE controller. (Partitions support up to 4 IDE devices, but one device must be the startup disk.)
    - A virtual DVD drive can access CDs and DVDs, either .iso files or physical media. However, only one partition can be configured to access a physical CD/DVD drive at a time.
- Virtual COM Port
    - Each partition is configured with 2 virtual serial (COM) ports that can be attached to a named pipe to communicate with a local or remote physical computer.

    Important: No access to a physical COM port is available from a partition.
- Virtual Floppy Drive
    - Each partition is configured with 1 virtual floppy drive, which can access virtual floppy disk (.vfd) files.

    Important: No access to a physical floppy drive is available from a partition.

3.1.2.3 Supported Guest Operating Systems

The following operating systems are supported for use in a partition as a guest operating system. 32-bit and 64-bit guest operating systems can be executed at the same time on one server running Hyper-V. Note that Hyper-V does not make any security-related assumptions based on the type of guest operating system used. Therefore, other operating systems not explicitly listed bellow, such as future versions of the listed ones, may also be used as guests.

- The following 32-bit and 64-bit editions of Windows Server 2008 can be used as a supported guest operating system in a partition configured with 1, 2, or 4 virtual processors:
    - Windows Server 2008 Standard and Windows Server 2008 Standard without Hyper-V
    - Windows Server 2008 Enterprise and Windows Server 2008 Enterprise without Hyper-V
    - Windows Server 2008 Datacenter and Windows Server 2008 Datacenter without Hyper-V
    - Windows Web Server 2008
    - Windows Server 2008 HPC Edition

- The following editions of Windows Server 2003 can be used as a supported guest operating system in a partition configured with 1 or 2 virtual processors:
    - Windows Server 2003 R2 Standard Edition with Service Pack 2
    - Windows Server 2003 R2 Enterprise Edition with Service Pack 2
    - Windows Server 2003 R2 Datacenter Edition with Service Pack 2
    - Windows Server 2003 Standard Edition with Service Pack 2
    - Windows Server 2003 Enterprise Edition with Service Pack 2
    - Windows Server 2003 Datacenter Edition with Service Pack 2
    - Windows Server 2003 Web Edition with Service Pack 2
    - Windows Server 2003 R2 Standard x64 Edition with Service Pack 2
    - Windows Server 2003 R2 Enterprise x64 Edition with Service Pack 2
    - Windows Server 2003 R2 Datacenter x64 Edition with Service Pack 2
    - Windows Server 2003 Standard x64 Edition with Service Pack 2
    - Windows Server 2003 Enterprise x64 Edition with Service Pack 2
    - Windows Server 2003 Datacenter x64 Edition with Service Pack 2
- The following versions of Windows 2000 can be executed in a partition configured with 1 virtual processor:
    - Windows 2000 Server with Service Pack 4
    - Windows 2000 Advanced Server with Service Pack 4
- The following Linux distributions can be executed in a partition configured with 1 virtual processor:
    - Suse Linux Enterprise Server 10 with Service Pack 2 (x86 edition)
    - Suse Linux Enterprise Server 10 with Service Pack 2 (x64 edition)
    - Suse Linux Enterprise Server 10 with Service Pack 1 (x86 edition)
    - Suse Linux Enterprise Server 10 with Service Pack 1 (x64 edition)
- The following 32-bit and 64-bit versions of Windows Vista can be executed in a partition configured with 1 or 2 virtual processors:

- Windows Vista Business with Service Pack 1
- Windows Vista Enterprise with Service Pack 1
- Windows Vista Ultimate with Service Pack 1
- The following versions of Windows XP can be executed in a partition:
- Windows XP Professional with Service Pack 3 (configured with 1 or 2 virtual processors)
- Windows XP Professional with Service Pack 2 (configured with 1 virtual processor)
- Windows XP Professional x64 Edition with Service Pack 2 (configured with 1 or 2 virtual processors)

3.1.2.4 Integration Services (Enlightenments)

Integration services are available for supported guest operating systems as described in the following table.

Guest operating system	**Device and service support**
Windows Server 2008 (64-bit editions)	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2008 (x86 editions)	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2003 (x64 editions) with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Server 2003 (x86 editions) with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows 2000 Server with Service Pack 4	Drivers: IDE, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, and heartbeat

Guest operating system	Device and service support
Windows 2000 Advanced Server with Service Pack 4	Drivers: IDE, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, and heartbeat
Suse Linux Enterprise Server 10 (x64 edition) with Service Pack 1 or 2	Drivers only: IDE, SCSI, networking, and mouse
Suse Linux Enterprise Server 10 (x86 edition) with Service Pack 1 or 2	Drivers only: IDE, SCSI, networking, and mouse
Windows Vista (64-bit editions) with Service Pack 1	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows Vista (x86 editions) with Service Pack 1	Drivers: IDE, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, heartbeat, and online backup
Windows XP Professional (x86 editions) with Service Pack 2 or 3	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, and heartbeat
Windows XP Professional x64 Edition with Service Pack 2	Drivers: IDE, SCSI, networking, video, and mouse Services: operating system shutdown, time synchronization, data exchange, and heartbeat

3.2 How to Obtain the CC-Evaluated Product

The Common Criteria evaluation of Microsoft Hyper-V Server 2008 has assessed the distribution method for the evaluated version of the TOE to ensure that a distribution path is available that allows users to verify the authenticity of the software. The distribution covered by this evaluation is via electronic download. The following steps describe how to obtain the evaluated version of Microsoft Hyper-V Server 2008 via the Internet and how to verify its authenticity.

3.2.1 Windows Platform Common Criteria Certifications

General information about the evaluation of this and other Microsoft Windows products can be obtained at http://technet.microsoft.com/en-us/dd229319.aspx.

3.2.2 Hyper-V Evaluation Configuration Guide

This document should be obtained from the Windows Platform Common Criteria Certifications Site:

http://technet.microsoft.com/en-us/dd229319.aspx.

Administrators who wish to run the validated configuration must first validate the authenticity and integrity of the guidance provided in this document by sending an e-mail to wincc@microsoft.com and requesting a digitally signed copy of this guide. Authorized Microsoft personnel will respond with a digitally signed s-mime message containing this guide. Administrators must verify the digital signature of the message and use the guide included in the response. Most e-mail clients have built-in means for verifying the digital signature of s-mime messages.

3.2.3 Microsoft Hyper-V Server 2008 – English

The ISO image for Microsoft Hyper-V Server 2008 can be obtained from the following URL:

http://www.microsoft.com/downloads/details.aspx?FamilyId=6067CB24-06CC-483A-AF92-B919F699C3A0&displaylang=en

Since this download is not SSL/TLS-protected, additional steps must be followed to verify its authenticity. Please refer to section 3.2.5 for verifying the SHA-1 hash of the ISO file.

3.2.4 Hotfix

The Hyper-V Update for Windows Server 2008 (KB950050) can be obtained from the following URL:

http://www.microsoft.com/downloads/details.aspx?FamilyId=6F69D661-5B91-4E5E-A6C0-210E629E1C42&displaylang=en

When you install this Hotfix, the Windows Update mechanism will automatically verify the digital signature for this package in order to ensure that it has been signed by Microsoft. In addition, the SHA-1 hash value for the file is provided in section 3.2.5.

3.2.5 Verifying SHA-1 hash sums

SHA-1, a cryptographic hash sum mechanism, should be used to verify the authenticity of the downloaded installation files by computing a message digest of the downloaded file and comparing it with the hash values identified below.

On an existing installation of Windows Server, the following command can be executed at the command prompt in order to generate a SHA-1 hash over the file represented by <filename>:

certutil -hashfile <filename>

On other operating platforms, a variety of free, publicly available utilities can be used, including:

- Microsoft's File Checksum Integrity Verifier can be obtained at http://support.microsoft.com/default.aspx?scid=kb;en-us;841290. The command to be executed would be:

  fciv -sha1 <filename>

The hash sums for the downloaded ISO image and Hotfix are as follows:

File name	*SHA-1 hash*
ServerHyper_MUIx2-080912.iso	1073 1C30 27A0 352A B4FF 5F7A 575B 0287 6531 0C38
Windows6.0-KB950050-x86.msu	CA9C 1923 5F47 8974 3D1D 818C 3372 6E0F 2600 238A

3.3 Evaluated and Non-Evaluated Security Functionality

3.3.1 Evaluated Security Functionality

3.3.1.1 Evaluated Security Functionality Provided by Hyper-V Components

3.3.1.1.1 Generation of Hyper-V audit records

The hypervisor layer and other Hyper-V components in the root partition are able to generate auditable events. Those events are stored and managed by the Server 2008 audit function. Security relevant events generated by the hypervisor are signaled to the root partition and the root partition generates and records the audit record for those events. The security relevant events signaled by the hypervisor are:

- The creation of a partition
- The deletion of a partition
- A failure condition detected internal to the hypervisor component

In addition to those events the Hyper-V specific components within the root partition are capable to generate audit records for the following events:

- Modifications to the Hyper-V AzMan policy
- Access checks performed by AzMan

Each audit records is sent to the Event Logger in the Server 2008 Server Core in the root partition, which inserts the time and data and stores the record in the event log.

3.3.1.1.2 Security Management Functionality

Hyper-V can be managed either directly using the management functions within the root partition, or remotely using a client that connects to the WMI and performs the management activities using this interface. In both cases the administrative user that wants to perform management activities is authenticated by the Server 2008 authentication function and gets his Server 2008 managed privileges assigned. Those define the management activities he is allowed to perform.

Hyper-V specific configuration data is stored in objects that are protected by the standard Server 2008 access control functions. Access to those objects is therefore managed by the access control management functions of Server 2008.

Hyper-V uses the "Authorization Manager" (AzMan) to define a role-based access control model for managing Hyper-V. The root partition protects a set of Hyper-V management operations. A default scope is provided as well as the set of operations that can be controlled. Tasks and roles can be defined by an application that uses the AzMan API for the management of the policy store. The HVRemote.wsf and HVRoles.wsf command line scripts must be used to manage the authorization store of the AzMan policy for Hyper-V.

> **Important** Administrators who wish to run the validated configuration must first validate the authenticity and integrity of the guidance provided in this document by sending an e-mail to wincc@microsoft.com and requesting a digitally signed copy of this guide.

The authorization store for Hyper-V can be found in the file "C:\ProgramData\Microsoft\Windows\Hyper-V\Initialstore.xml" in the root partition. This file needs to be selected when defining or editing role definitions, defining or editing task definitions, or defining or editing scopes. Roles can then be assigned to users, defining the management activities they are allowed to perform.

The authorization policy for Hyper-V has a set of operations which can be used to group to tasks and/or be assigned to roles. Those are:

- Operations on Hyper-V services
    - Read Service Configuration
    - Reconfigure Service
    - View Virtual Switch Management Service
- Operations on Virtual Machines
    - Create Virtual Machine
    - Delete Virtual Machine
    - Change Virtual Machine Authorization Scope
    - Start Virtual Machine
    - Stop Virtual Machine
    - Pause and Restart Virtual Machine
    - Reconfigure Virtual Machine

  - View Virtual Machine Configuration
  - Allow Input to Virtual Machine
  - Allow Output from Virtual Machine
- Operations on Virtual Switches
  - Create Virtual Switch
  - Delete Virtual Switch
  - Modify Switch Settings
  - View Switches
  - Create Virtual Switch Port
  - Delete Virtual Switch Port
  - Connect Virtual Switch Port
  - Disconnect Virtual Switch Port
  - Modify Switch Port Settings
  - View Switch Ports
  - View LAN Endpoints
  - Change VLAN Configuration Port
  - View VLAN Settings
  - Create Internal Ethernet Port
  - Delete Internal Ethernet Port
  - View Internal Ethernet Port
  - Bind External Ethernet Port
  - Unbind External Ethernet Port
  - View External Ethernet Ports

Whenever a user attempts to perform an administrative operation on Hyper-V, the AzMan interfaces for checking access are called to validate the user's rights to perform the management function.

3.3.1.1.3 Internal Protection Functionality

Hyper-V protects its own binary code and data by maintaining separate address spaces for those that are protected from access or unmediated interference by un-trusted subjects or subjects outside of the Hyper-V Server Role on Server Core 2008 that may communicate with the Hyper-V Server Role via its network interfaces. The main purpose of the internal protection functionality of Hyper-V is the maintenance of this separate address spaces and the mediation of all references to its secure data and protected user data. Hyper-V protects each guest partition from unauthorized interference by other guest partitions.

3.3.1.1.4 Resource Utilization Functionality

Hyper-V provides functions that allow an authorized administrator to define the maximum amount of memory and CPU time a guest partition or a subject within a guest partition is allowed to use. Hyper-V controls the use of those resources and ensures that a given guest partition does not use more of those resources than allocated to the partition. This prohibits that a single guest partition consumes all resources of a specific type and thereby cause a denial of service for other guest partitions.

3.3.1.2 Evaluated Security Functionality Provided By Windows Server 2008 Core

As described above the root partition consists of a Server Core installation of Server 2008 with the Hyper-V specific components described above as being part of the root partition. In addition to those, the TOE also relies on non Hyper-V specific components within the root partition. The security functions provided by those non Hyper-V specific components are:

- Identification and authentication of administrative users
- Management of the security attributes of administrative users
- Access control policy for Server 2008 files and objects
- Management of the Server 2008 access control policy
- Generation of audit events specific for Server 2008
- Management and protection of the audit trail
- Review of audit records
- Management of date and time

The Hyper-V server role requires each administrative user to be identified and authenticated prior to performing Hyper-V-mediated functions on behalf of that user. Administrative users are identified and authenticated by the root partition using the regular identification and authentication function implemented in Server 2008 Core.

3.3.1.2.1 Identification and Authentication of Administrative Users

The Hyper-V server role requires each user to be identified and authenticated prior to performing Hyper-V-mediated functions on behalf of that user, with a few exceptions, regardless of whether the user is logging on interactively or is accessing the system via a network connection.

For initial interactive logon, a user must invoke a trusted path in order to ensure the protection of identification and authentication information. The trusted path is invoked by using the Ctrl+Alt+Del key sequence, which is always captured by the Server Core 2008 (i.e., it cannot be intercepted by an un-trusted process), and the result will be a logon dialog that is under the control of the Server Core 2008. Once the logon dialog is displayed, the user can enter their identity (username and domain) and authentication (password).

Users can change their password either during the initial interactive log or while logged on. To change a user's password, the user must invoke the trusted path by using the Ctrl+Alt+Del key sequence. The logon dialog displayed allows the user to select an option to change their password. If selected, a change password dialog is displayed which requires the user to enter their current password and a new password.

The Server Core 2008 will change the password only if the Server Core 2008 can successfully authenticate the user using the current password that is entered.

3.3.1.2.2 Management of Security Attributes of Administrative Users

The Server Core 2008 in the root partition maintains databases (collectively referred to as user attribute database) that fully define user and group accounts. These definitions include:

- Account name – used to represent the account in human-readable form;
- SID – a User Identifier (UID) or group identifier used to represent the user or group account within the TOE;
- Password (only for user accounts) – used to authenticate a user account when it logs on (stored in hashed form and is encrypted when not in use using a Rivest's Cipher (RC)4 algorithm and a RC4 system generated key);
- Groups – used to associate group memberships with the account
- Privileges – used to associated TSF privileges with the account;
- Logon rights – used to control the logon methods available to the account (e.g. the "logon locally" right allows a user to interactively logon to a given system);
- Miscellaneous control information – used to keep track of additional security relevant account attributes such as allowable periods of usage, whether the account has been locked, whether the password has expired, password history, and time since the password was last changed; and,

- Other non-security relevant information – used to complete the definition with other useful information such a user's real name and the purpose of the account or to support functions not used in the evaluated configuration.

The Server Core 2008 provides a set of functions that allow the account policy to be managed. These functions include the ability to define account policy parameters, including minimum password length. The minimum password length can be configured to require a minimum set of characters – see Section 5.1.1.5. However, the administrator guide recommends that the minimum password length be configured to no less than eight (8) characters (with at least 90 available characters, the password space is 4,304,672,100,000,000 available combinations). Therefore, in the evaluated configuration, the probability that a random attempt will succeed is less than one (1) in 5x1015; for multiple attempts within one minute, the probability that a random attempt will succeed is less than one (1) in 25x1012.

During authentication, Server Core 2008 does not provide feedback that will reduce the probability below the metrics identified above. Furthermore, Server Core 2008 forces a delay between attempts, such that there can be no more than ten (10) attempts per minute.

For each subsequent failed logon following five (5) consecutive failed logon occurrences in the last 60 seconds, the function sleeps for 30 seconds before showing a new logon dialog. It therefore supports the I&A function that no more than ten (10) interactive logon attempts are possible in any 60 second (one minute) period.

3.3.1.2.3 Access Control Policy for Server Core 2008 Files and Objects

The Server 2008 Server Core instance in the root partition mediates access between subjects and user data objects, also known as named objects. Subjects consist of processes with one or more threads running on behalf of users, which in the case of the root partition are either the administrative users or the worker processes (which have their own Security Identifier).

Tokens contain the security attributes for a subject. Tokens are associated with processes and threads running on behalf of the user. The DAC related information in the token includes: the SID for the user, SIDs representing groups for which the user is a member, privileges assigned to the user, an owner SID identifying SID to assign as owner for newly created objects, a default DACL (for newly created objects), token type (primary or impersonation), impersonation level (for impersonation tokens), an optional list of restricting SIDs, and a logon ID for the session.

Every object has a unique Security Descriptor (SD) that includes an ACL. SDs contain all of the security attributes associated with an object. All objects covered by the access control policy have an associated SD. The security attributes from a SD used for access control are the object owner SID, the DACL present flag, and the DACL itself, if present.

DACLs contain a list of Access Control Entries (ACEs). Each ACE specifies an ACE type, a SID representing a user or group, and an access mask containing a set of access rights. Each ACE has inheritance attributes associated with it that specify if the ACE applies to the associated object only, to its children objects only, or to both its children objects and the associated object.

3.3.1.2.4 Management of Access Control Policy

The notion of role within Server Core 2008 is generally realized by assigning group accounts and privileges to a given user account. Whenever that user account is used to logon, the user will be assuming the role that corresponds with the combination of groups and privileges that it holds. While additional roles could be defined, the CC-evaluated configuration defines just one logical role: the Authorized Administrator role.

The Administrator role is defined as any user account that is assigned one of the security-relevant privileges for managing the configuration of the partitions or to manage users and groups.

3.3.1.2.5 Generation of Audit Events

The Event logger service of Server Core 2008 creates the security event log, which contains the security relevant audit records collected on a system. For each audit event, the Event Logger stores the following data in each audit record:

- Date: The date the event occurred.
- Time: The time the event occurred.
- User: The security identifier (SID) of the user on whose behalf the event occurred that represents the user.
- Event ID: A unique number identifying the particular event class.
- Types: Indicates whether the security audit event recorded is the result of a successful or failed attempt to perform the action.

The Server Core 2008 in the root partition maintains an audit policy in its database that determines which categories of events are actually collected. Defining and modifying the audit policy is restricted to the authorized administrator.

The authorized administrator can select events to be audited by categories to be audited. An authorized administrator can individually select each category.

In addition to the system-wide audit policy configuration, it is possible to define a per-user audit policy. This allows individual audit categories (of success or failure) to be enabled or disabled on a per user basis.

3.3.1.2.6 Management and Protection of the Audit Trail

The Event Logger controls and protects the security event log. To view the contents of the security log, the user must be an authorized administrator. The security event log is a system resource, created during system startup. No interfaces exist to create, destroy, or modify a security event within the security event log.

The TSF protects against the loss of events through a combination of controls associated with audit queuing and event logging. As configured in the TOE, audit data is appended to the audit log until it is

full. The TOE protects against lost audit data by allowing the authorized administrator to configure the system to generate an audit event when the security log reaches a specified capacity percentage (e.g., 90%).

Additionally, the authorized administrator can configure the system not to overwrite events and to shutdown when the security log is full. When so configured, after the system has shutdown due to audit overflow, only the authorized administrator can log on. When the security log is full, a message is written to the terminal display of the authorized administrator indicating the audit log has overflowed.

Audit events may be lost if the audit event queues reach their high-water mark, or if the security log file is full. The TOE can be configured to crash when the audit trail is full. The security log file is limited in size by the resources available on the system.

3.3.1.2.7 Review of Audit Records

The event viewer administrator tool provides a user interface to view, sort, and search the security log. The security log can be sorted and searched by user identity, event type, date, time, source, category, event ID, and computer. The security log can also be searched by free form texts occurring in the audit records.

Reading and evaluation of the audit trail is restricted to administrators authorized to access the audit trail. They have tools available that allow them to transform the audit records to human readable format and further evaluate the records.

3.3.1.2.8 Management of Date and Time

Each hardware platform supported by the CC-evaluated configuration specified in Section 3.1 includes a real-time clock. The real-time clock is a device that is assigned to the root partition and can only be accessed using functions provided by the Server Core 2008. Specifically, Server Core 2008 provides functions that allow users, including the Server Core 2008 itself and the Hyper-V server role, to query and set the clock, as well as functions to synchronize clocks within a domain. The ability to query the clock is unrestricted, while the ability to set the clock requires a privilege dedicated to that purpose. This privilege is only granted to authorized administrators to protect the integrity of the time service.

3.3.2 Non-Evaluated Security Functionality

This section lists the security functionality that was determined to be out of scope and therefore not evaluated for the Hyper-V Server Role. You can use the functionality listed in this section; however, the current Common Criteria evaluation for Hyper-V Server role does not provide any level of assurance for the use of these items:

- Smart card authentication of users
- Windows Cryptographic Service Providers
- Windows® Encrypted File System (EFS)
- Windows® BitLocker™ Drive Encryption
- Windows® Trusted Platform Module (TPM)

- SSL/TLS-based encryption of network connections
- Extended AzMan Role Based Access Control functionality outside the subset required to manage the Hyper-V Policy Store.

4 Security Policy Assumptions and Conditions

A CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 Core makes specific assumptions about the required security policy and installation restrictions. Assumptions are items and issues that cannot be formally evaluated under CC but are required to ensure the security level of a CC-evaluated system. Therefore, to reproduce the CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 Core, you must review and apply the items in this chapter.

This chapter covers the following topics:

- Security Policy Assumptions
- Installation and Configuration Constrains

4.1 Security Policy Assumptions

The Microsoft Windows Server 2008 Hyper-V Security Target (http://www.commoncriteriaportal.org/products_ALL.html) specifies security policy assumptions for the target of evaluation (TOE) on which the evaluation of the TOE is based. Therefore, to comply with the CC-evaluated system, enforcing and maintaining the conditions defined in the assumptions listed below is mandatory.

4.1.1 Assumptions on the System Environment

It is assumed that the non-IT environment provides the TOE with appropriate physical security commensurate with the value of the IT assets protected by the TOE.

4.1.2 Assumptions on System Administrators

Authorized administrators of the TOE are assumed to be knowledgeable and trustworthy to follow this guidance and not misuse their privileges.

It is assumed that properly trained trusted administrators will create and manage the configuration data of partitions.

It is assumed that the administrator installs and configures the TOE in accordance with the guidance provided for the installation and configuration of the TOE.

4.1.3 Assumptions on Connectivity and Remote Administration

It is assumed that remote administration is performed only using properly protected communication links.

It is also assumed that any other IT product that may be used to support the authentication of administrators, used to protect communication links, or used to assist administrators in their

administrative tasks is trusted to perform its security related functions correctly and does not include side effects that may allow unauthorized persons to perform administrative functions on the TOE or perform administrative functions other than those explicitly initiated by the trusted administrator.

4.1.4 Assumptions on Partition User Connectivity

It is assumed that the IT environment is configured in a way that allows users provisioned and entitled to connect to a specific partition, other than the root partition, to do so and access all the information contained within the partition in strict correspondence to the rights assigned to each user. Note that Hyper-V ensures partition isolation that prevents users from one partition to interfere with users or resources from another partition – see Section 3.3.1.1.3.

4.1.5 Assumptions on Software

It is assumed that no additional software than the one specified in the configuration guidance is installed in the root partition of Hyper-V.

4.1.6 Assumptions on Hardware

It is assumed that the underlying hardware of the TOE operates correctly as described in the hardware manuals and does not expose undocumented critical side effects.

4.1.7 Assumptions on Memory Management

It is assumed that the Windows Server 2008 instance which is running in the root partition provides memory management services to other components running in the server instance or the root partition with kernel-mode privileges. The assumption also covers that a dedicated and functionally-complete kernel memory management API to these components is exposed; in particular, the kernel memory manager ensures that any new request for allocating memory coming through the API is serviced by zeroizing the memory pages before making them available to the requestor.

4.2 Installation and Configuration Constraints

4.2.1 Installing the TOE

Administrators installing the system must follow the step-by-step procedure outlined in the Server Core Installation Option Getting Started Guide (http://technet.microsoft.com/en-us/library/cc753802.aspx) for Windows Server 2008.

> **Important** Administrators are strongly advised when following this procedure not to configure the firewall with the example command `netsh advfirewall set rule group="Remote Administration" new enable=yes` shown at the guide – see also Section 5.1.2.6. Using this command will result in enabling security-relevant interfaces that have not undergone a CC evaluation and therefore will result in a non-evaluated configuration with possibly reduced security.

Once the server installation is complete, enable the Hyper-V role by issuing the following command at a command prompt:

```
start /w ocsetup Microsoft-Hyper-V
```

> **Important** Before you enable the Hyper-V role, ensure that you have enabled the required hardware-assisted virtualization and hardware-enforced Data Execution Prevention (DEP) BIOS settings.

Administrators are advised to familiarize themselves with and follow the guidance in Chapter 1 of Hyper-V™ Security Guide (http://go.microsoft.com/fwlink/?LinkId=92552) for setting up the Hyper-V role using default installation options that result in minimal attack surface.

> **Important** Chapter 2 in Hyper-V™ Security Guide introduces ways for delegating the management of virtual machines. Administrators must not attempt to configure any of the tools described in this section. Instead, the installing administrators must follow the procedure in Section 5.2 of this document.

4.2.2 Verifying the TOE version

In order to verify that the installed version of the TOE in fact matches the evaluated version of the TOE as identified in Section 3.1, the following command can be executed at the command prompt:

systeminfo

The OS Version and list of installed Hotfixes should match the information provided above.

5 Configuring Elevated Security Functionality

A CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 Core makes specific assumptions about the security functionality included in the evaluation. To install and configure a CC-evaluated implementation of the Hyper-V server role of Windows Server 2008 Core, you must first use the standard technical documentation and guidance for the product introduced in Section 4.2. Then you must review and apply the items in this chapter.

This chapter covers the following topics

- Hardening Windows Server 2008 Core
- Hardening the Hyper-V Server Role

5.1 Hardening Windows Server 2008 Core

5.1.1 Secure Initial System Configuration

Administrators must ensure that the following Windows services/features are disabled:

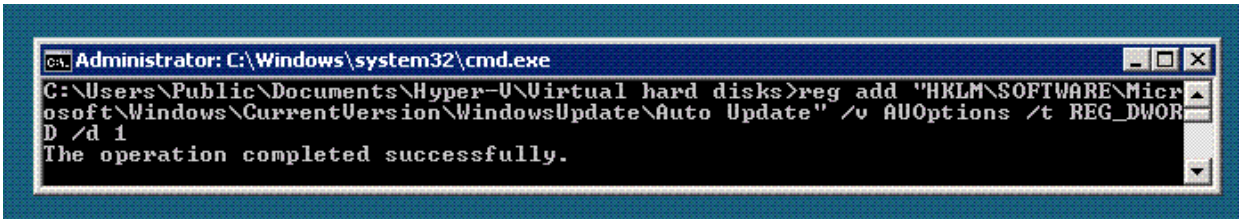
- File sharing on disabled by default. It must not be enabled.
- Firewire connection at BIOS on the host machine must be disabled.
- Failover clustering is disabled by default and must be kept disabled during normal operation.

5.1.1.1 Add/Remove Windows Updates

The CC evaluation of the Hyper-V server role of Windows Server 2008 was performed on the specific configuration defined in this guide. Note that this covers the use of additional hardware device drivers. Any deviation from this configuration may result in a non-evaluated system, but does not necessarily mean that the security of the resulting system is reduced. Therefore, it is the responsibility of the

individual organization to determine the potential risks and benefits associated with installing newer Windows updates or additional software that was not subject to this evaluation. Consequently, the recommended setting for Windows Update on the Server Core 2008 installation is to disable auto updates. To accomplish this, use the `reg` command as follows:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto
Update" /v AUOptions /t REG_DWORD /d 1
```



5.1.1.2 Install Server Roles

No server roles other than the Microsoft-Hyper-V role installed according to the instructions in Section 4.2.1 should be installed on the system.

5.1.1.3 Review Windows Services

The evaluated configuration supports only the services established during the default installation and configuration of the system defined in Section 4.2.1. Administrators of the server are advised to monitor the set of running services on the system through the Task Manager UI on Server Core 2008. Type

```
taskmgr
```

in a command prompt. This causes the Task Manager UI to pop up. Then select the Services tab and view the services installed on the system and their current status. Administrators are advised to keep a record of the list of services and their status upon installation completion.

5.1.1.4 Creating Additional Accounts for Administrators

Administrators on standalone installations must resort to the commands

```
net accounts
net localgroup
net user
```

for managing local users and groups. Only administrative accounts consistent with the assumptions in Sections 4.1.2 and 4.1.3 are allowed.

Domain administrators must provision new administrative accounts on other computers connected to the same domain using the standard Windows tools for managing domain security policy, users and groups. Note that such administration is external to the configuration established in this guide. The resulting policy and user account information is imported as read-only on the Server Core 2008 and applied locally.

Important Installations joined to a domain must only be administered indirectly by domain administrators managing the domain policies.

5.1.1.5 Configuring the Default Security Policy

Administrators on standalone installations must resort to the command line utility

```
secedit
```

for managing the default security policy. See Section 5.1.3.1 for instructions how to export and review the default security policy. Administrators must ensure that the [System Access] portion is at least as strong as the setup shown below:

```
[System Access]
MinimumPasswordAge = 0
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 0
LockoutBadCount = 0
RequireLogonToChangePassword = 0
ForceLogoffWhenHourExpire = 0
NewAdministratorName = "Administrator"
NewGuestName = "Guest"
ClearTextPassword = 0
LSAAnonymousNameLookup = 0
EnableAdminAccount = 1
EnableGuestAccount = 0
```

See Section 5.1.3.3 for details on how to set the local security policy on the machine.

Domain administrators must administer the default security policy on the domain using other computers connected to the same domain using the standard Windows tools for managing domain security policy. Note that such administration is external to the configuration established in this guide. The resulting security policy is imported as read-only on the Server Core 2008 and applied locally.

> **Important** Installations joined to a domain must only be administered indirectly by domain administrators managing the domain security policy.

5.1.2 Secure System Operation

5.1.2.1 System Startup, Shutdown, and Crash Recovery

The installation of Server Core 2008 is contained in a secure non-IT environment according to Section 4.1.1. Nevertheless, administrators must inspect the system audit logs and review any security anomaly as a result of system startup, shutdown, and crash recovery.

5.1.2.2 Editing Windows Registry Settings

Administrators must edit Windows registry settings with extreme care because this may undesired system behavior and result in a non-evaluated configuration.

5.1.2.3 Installation of Additional Software

Administrators must **not** install any additional software, according to Section 4.1.5. Any deviation from this configuration may result in a non-evaluated system, but does not necessarily mean that the security of the resulting system is reduced. Therefore, it is the responsibility of the individual organization to determine the potential risks in cases where additional software is needed.

5.1.2.4 Managing User Accounts

Administrators on standalone installations must resort to the commands

```
net accounts
net localgroup
net user
```

for managing local users and groups. Only administrative accounts consistent with the assumptions in Sections 4.1.2 and 4.1.3 are allowed.

5.1.2.5 Configuring Access Control for Files and Folders

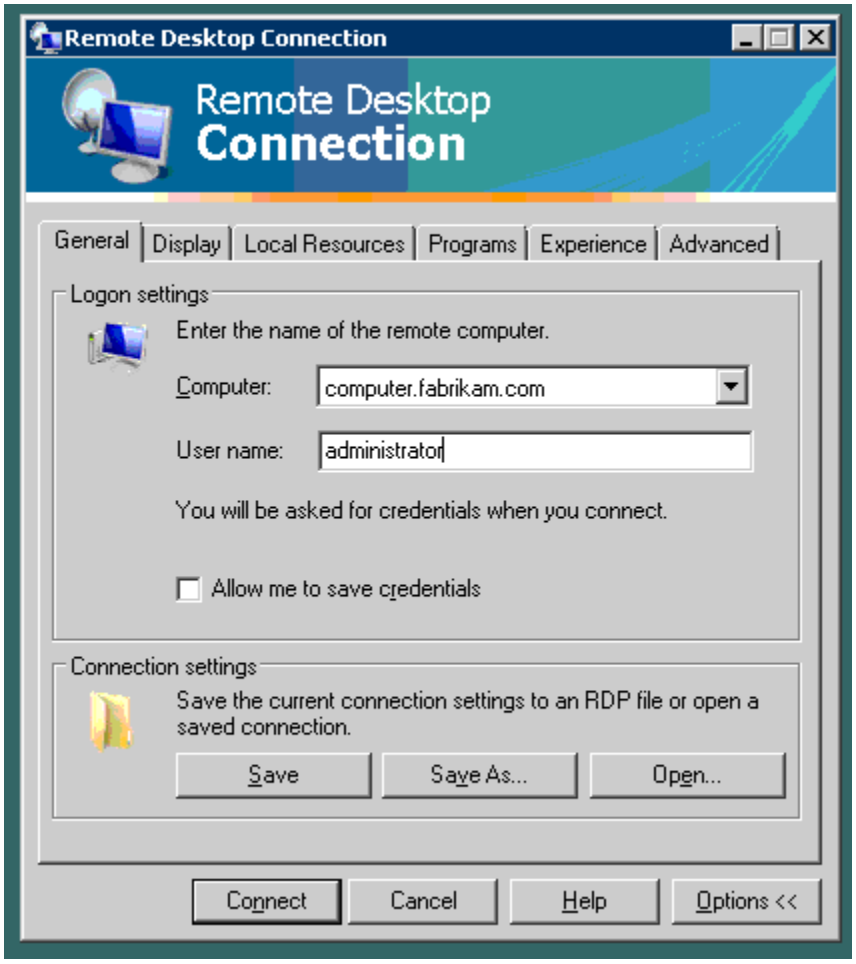
Administrators are advised to follow the guidance in Chapter 3 in Hyper-V™ Security Guide (http://go.microsoft.com/fwlink/?LinkId=92552) for details on how to configure the access control to all relevant files for the proper operation of the Hyper-V role.

5.1.2.6 Network and Firewall Connection

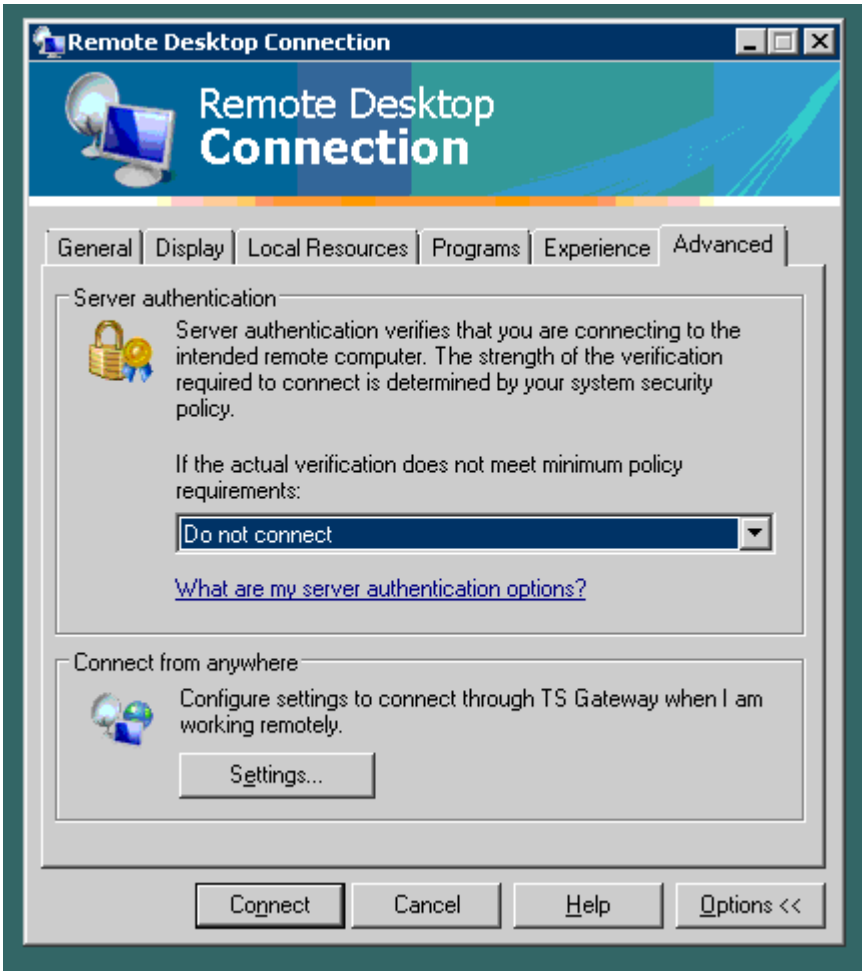
The network and firewall settings should support only the minimal set of services required to support the Hyper-V role. Only the configurations established in Sections 4.2.1, 5.1.3, and 5.2 must be established.

5.1.2.7 Using Terminal Services and Remote Desktop Connection

Administrators are required to use tools for remote management in strict compliance with the assumptions in Section 4.1.3. An example of such a tool is the Windows Remote Desktop Utility shown in the picture below.



When connecting from a remote location outside the boundaries of the corporate intranet, administrators are advised to use the Remote Desktop Connection under Virtual Private Network connection. For maximum security, administrators are advised to optionally verify that the server authentication connection option is enabled, as shown in the figure below, provided that the server has authentication credentials such as a PKI certificate. This security measure helps prevent connecting to a different computer or server than the one intended. This also prevents unintentional exposure of confidential information.

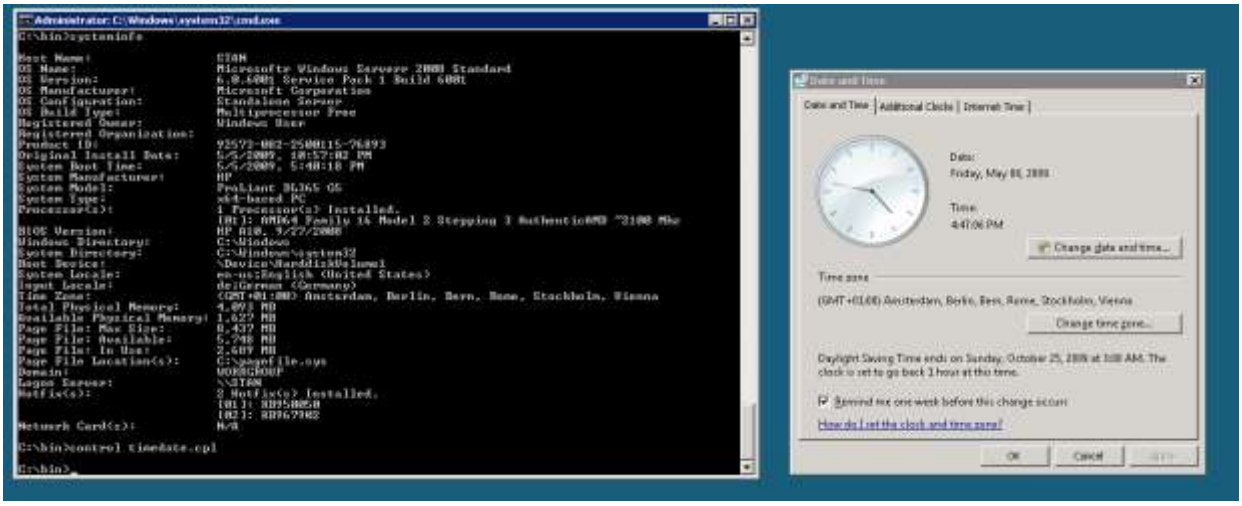


5.1.2.8 Setting the Windows System Time and Date

Setting the Windows System Time and Date is very important for maintaining the integrity of audit records. To accomplish this, issue the following command in a command prompt:

```
Control timedate.cpl
```

This will cause the Date and Time UI to popup and will allow you to set the date, time, and time zone.



5.1.3 Monitoring, Logging, and Audit

Administrators must first enable remote event log management on the Server Core 2008 instance using the following command:

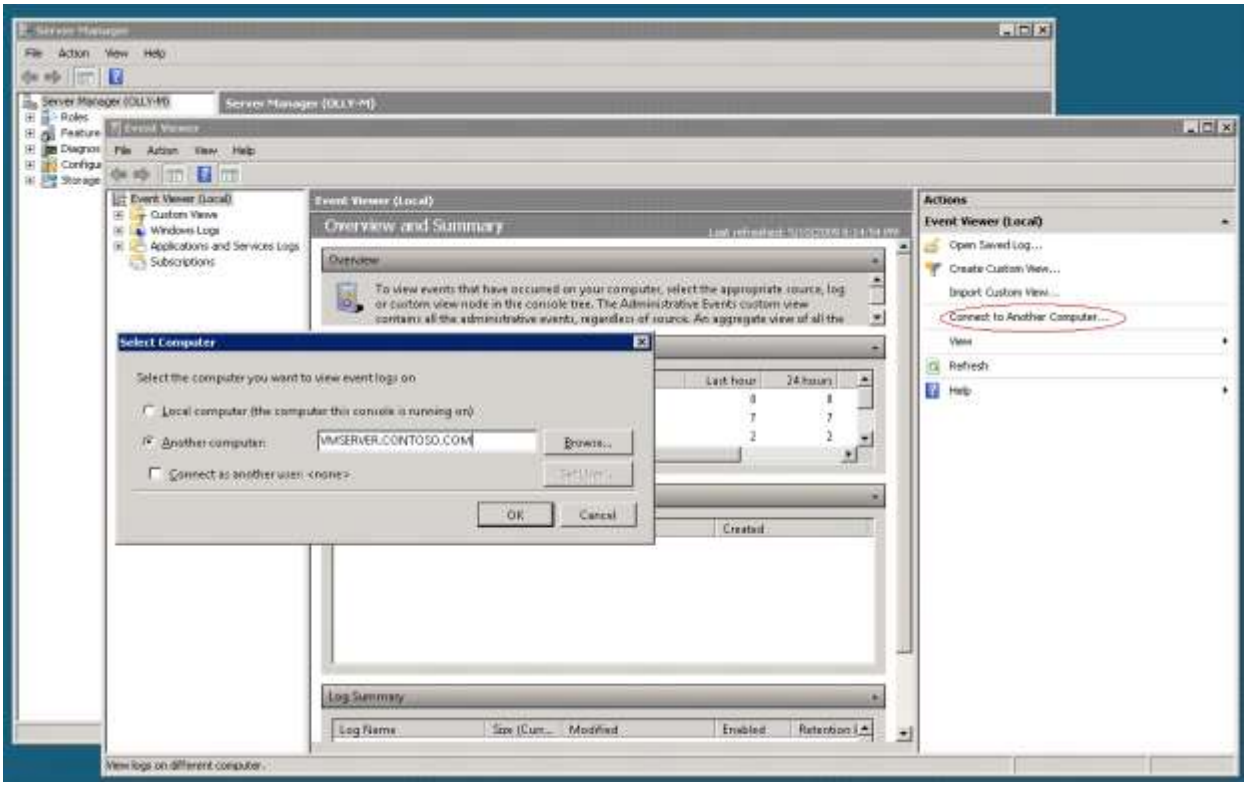
```
Netsh advfirewall firewall set rule group="Remote Event Log Management"
new enable=yes
```

Then, the administrators can review, configure, and monitor the event log using the Event Viewer MMC snap-in on a client machine by entering the following command in a command line prompt:

```
eventvwr.msc
```

Then, start the Event Viewer MMC snap-in (eventvwr.msc) from the remote workstation. Then, either click on the root node, labeled Event Viewer (Local), in the left pane, right-click and select "Connect to Another Computer "and point it to the server configured above or click the "Connect to Another Computer" action in the Actions pane – see the figure below.

Important This step must be performed **after** the Hyper-V Remote administration configuration is complete**.** See Section 5.2 for details.



5.1.3.1 Reviewing the System Configuration

To review the system configuration on a standalone server installation, including account policies, audit policies, type the following command in a command prompt:

```
secedit /export /cfg current_config.txt
```

Then view the output file current_config.txt with notepad.

For installations that are joined to a domain, view the domain security policy on a remote workstation joined to the same domain using elevated account privileges for the domain.

5.1.3.2 System Logging and Auditing

To display the events of a particular log, click a log from the list shown in the left pane of the Event Viewer MMC snap-in. To search for events within an event log, right-click on a particular log in the list shown in the left pane. Select “Filter Current Log”. This displays an UI that allows filtering the displayed events based on multiple criteria. The Create Custom View UI allows configuring the displayed events based on specific event source, logged time, task category, keywords, user, etc.

5.1.3.3 Configuring the Windows Audit Subsystem

Administrators must enable security event logging for both the Server Core 2008 and the Hyper-V server role in order to ensure the secure operation of the system. In particular, administrators must configure a strong audit policy and set the behavior of the system when the log file becomes nearly and completely full. Server Core 2008 allows configuration of a threshold value for generating a warning when the security log file reaches a certain size, as a percentage of the maximum allowed size of the security log

file. This warning helps administrators avoid disruptions of system operation. To configure the Windows Audit subsystem on a standalone server installation, perform the following four steps.

1. Edit the resulting current_config.txt from the command in Section 5.1.3.1 above.

    a. Set the [Even Audit] group values as follows:

    [Event Audit]

    ```
    AuditSystemEvents = 1
    AuditLogonEvents = 1
    AuditObjectAccess = 1
    AuditPrivilegeUse = 1
    AuditPolicyChange = 1
    AuditAccountManage = 1
    AuditProcessTracking = 1
    AuditDSAccess = 1
    AuditAccountLogon = 1
    ```

    b. Edit the registry entry controlling the LSA behavior upon audit failure in the [Registry Values] group by setting the following registry value:

    ```
    MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail=4,1
    ```

    c. Save the file.

    d. Set the new policy settings with the following command

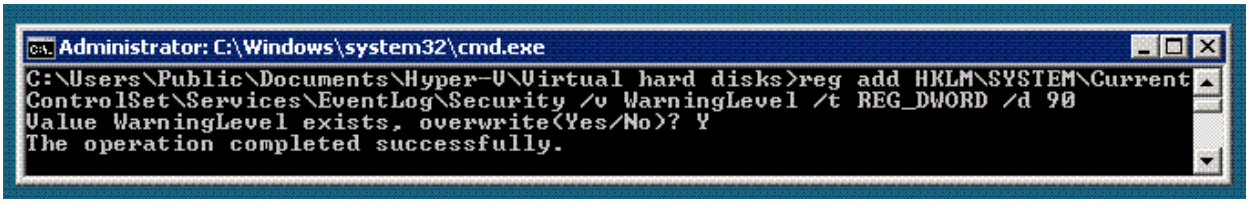
    ```
    secedit /configure /db current_config.db /cfg current_config.txt
    ```

2. Set a warning percentage threshold level for the security event log at which the system will generate a warning. To accomplish this, add the WarningLevel registry value **(**possible values: 0 to 100; recommended value: 90) to the key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\

    using the `reg` command:

    ```
    reg add HKLM\SYSTEM\CurrentControlSet\Services\EventLog\Security /v
    WarningLevel /t REG_DWORD /d 90
    ```

    See the figure below.



3. Reboot the system.

5.2 Hardening the Hyper-V Server Role

Administration of the Hyper-V server role can only be performed remotely. Administrators are required to follow the instructions in this section to enable the Hyper-V server role for remote administration.

5.2.1 Delegating Virtual Machine Management

Administrators must use the HVRemote.wsf script in order to configure for remote management. The procedure consists of server and remote client setup. It is provided in Section "Quick Start" in HVRemote Documentation 0.5-1.pdf.

> **Important** HVRemote has a built in capability to determine if there is a later version of HVRemote available. It uses Internet connectivity for this check to be made. Administrators should use the /noversioncheck option to turn off latest version verification. HVRemote will print an out-of-date version warning message but it should be ignored.

5.2.2 Role-based Access Control

Administrators must use the HVRoles.wsf script in order to configure roles for Hyper-V management, assign operations to them and link them to users.

The HVRoles script has the following commands:

```
' Add or remove task to authorization store
/addtask and /removetask
' Add or remove operation to authorization store
/addop and /removeop
' Add or remove role to authorization store
/addrole and /removerole
' Add or remove user to authorization store
/adduser and /removeuser
' Display the Authorization Store
/show
```

The typical steps to establish a new role and assign it to a user are as follows:

```
1. cscript hvroles.wsf /addtask:"New Task"
2. cscript hvroles.wsf /addop:"Some Operation" /assign:"New Task"
3. cscript hvroles.wsf /addrole"New Role" /assign:"New Task"
4. cscript hvroles.wsf /adduser:username /assign:"New Role"
```

In general, the operations must first be assigned to a Task and the Task should then be assigned to a Role. The user can then be assigned to this role. Hyper-V defines a set of 33 operations (see Chapter 2 in Hyper-V™ Security Guide (http://technet.microsoft.com/en-us/library/dd569113.aspx) for details about the defined operations.

> **Important** If the role already exists, /addrole will print a warning but should work fine to assign the corresponding task.

5.2.3 Protecting Virtual Machines

Administrators are advised to follow the guidance provided in Chapter 3 in Hyper-V™ Security Guide (http://technet.microsoft.com/en-us/library/dd569113.aspx).