IBM Intelligent Operations Center

IBM Intelligent Operations Center Cyber Hygiene Overview

Version 1 Release 5

IBM Intelligent Operations Center

IBM Intelligent Operations Center Cyber Hygiene Overview

Version 1 Release 5

Note
Before using this information and the product it supports, read the information in "Notices" on page 23.

This edition applies to IBM Intelligent Operations Center version 1, release 5, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2011, 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2011, 2012

Chapter 1. Cyber security

Securing the IT environment has long been a concern for national governments and is becoming increasingly important for critical infrastructure systems. Products and solutions providing critical infrastructure, such as IBM® Intelligent Operations Center, should, where possible, have known vulnerabilities removed before those products and solutions are made available.

Cyber security is risk mitigation, not risk prevention. Since IT systems must be running and accessible to provide value, there is always some risk that a system's information or control could be compromised. Cyber security consists of both static and dynamic elements. Cyber hygiene in IBM Intelligent Operations Center addresses the static elements of cyber security. Other tools and processes are needed to address the dynamic elements of cyber security. These tools and processes can include physical and personnel security procedures or network intrusion tooling.

The cyber hygiene capabilities provide by IBM Intelligent Operations Center are designed to address areas such as weak security configurations, software errors, system administration errors, and system security process errors. To provide this support, cyber hygiene provides installation and configuration features that configure the operating system and administration features that set secure settings and install key security-related fix packs. For example, systems are configured so no user IDs exist without a password and insecure Linux services, such as ftp, snmp, rlogin are disabled. However, systems cannot be automatically configured to meet specific enterprise security practices.

© Copyright IBM Corp. 2011, 2012

Chapter 2. Cyber hygiene overview

The cyber hygiene feature of IBM Intelligent Operations Center is designed to provide services remedying potential security exposures in the installed system.

Note: Commonly, the term "vulnerability" is used to refer to both security vulnerabilities and security exposures. Cyber hygiene defines a vulnerability as a programming error in an application that enables security breaches. Cyber hygiene defines an exposure as an operating system or application configuration selection that is less secure. Exposures can be addressed by choosing a more secure configuration option. For example, a directory can be configured to allow all users to store files there. It can also be configured more securely so that only the owner can store files in the directory.

Cyber hygiene has two key elements:

- Mitigation and correction of known security exposures in the Linux operating system and its associated users, directories, and files. It does this through a set of tools and scripts.
- Documentation of the assessment of almost 1000 known vulnerabilities and exposures in the operating system, products, and system configuration.

By handling security exposures during the installation process, less work is required by the customer to achieve an increased security level in the deployed system.

For example, a government agency can use the cyber hygiene remediation and documentation to help support certification and accreditation of the system for deployment on a secure network. Commercial business customers can use the same process to improve the security of their environment.

Cyber security provides risk mitigation, not risk prevention. Since systems must run and be accessible to provide value, there is always a risk that a system's information or its control can be compromised.

Cyber hygiene does not address application-specific vulnerabilities, which include how threats such as Denial of Service, SQL injection, and so on, are handled by the application. Instead, Cyber hygiene provides a foundation for application security by addressing user, directory, and file security exposures in a general way; not targeted to any specific application. Cyber hygiene is run after product installation to correct these general vulnerabilities for system and application users, directories, and files. Any application used with the Linux operating system must be separately assessed for application-specific vulnerabilities.

The catalog of known vulnerabilities and exposures used in cyber hygiene is based on unclassified, non-confidential checklists from the United States Defense Information Services Agency (DISA). The items on these lists are assessed for applicability to cyber hygiene. Scanning scripts search for and log instances of an exposure and then, where applicable, the log files are used as input for remediation scripts addressing the problem. A small subset of security findings require different handling.

© Copyright IBM Corp. 2011, 2012

Documentation listing known vulnerabilities in IBM Intelligent Operations Center components, and the actions taken by cyber hygiene to mitigate them, is provided by IBM Intelligent Operations Center.

Cyber hygiene checklists

Cyber hygiene uses checklists based on unrestricted Defense Information Systems Agency (DISA) checklists and periodic vulnerability alerts.

Checklist item analysis

Each vulnerability identified in the unrestricted Defense Information System Agency (DISA) checklist defines data related to the vulnerability.

The information provided for each vulnerability include the following:

- A unique identifier. The identifier is made up of a Security Implementation Technical Guide (STIG) ID and a Vulnerability Management System (VMS) key.
- A short name summarizing the vulnerability.
- The severity of the vulnerability. Severity levels documented are:

  I High severity

  II Medium severity

  III Low severity
- The affected product or products.
- The affected product version or versions.
- A description of the vulnerability including any use cases, context, or interactions with other software.
- Any recommended actions. If remediation is not available through a patch or an upgrade, a recommended mitigation might be included.
- Any alert that the alert supersedes.

For each vulnerability it is important to understand whether or not it affects IBM Intelligent Operations Center. For example:

- Is the product release and fix level included with IBM Intelligent Operations Center affected? An earlier product release or fix might not be affected since the issue could have been introduced in a later release or fix.
- Is the product included with IBM Intelligent Operations Center being used in a way that exposes the vulnerability? For example, a problem might only exist when the product is using services from another product. If those services are unused in the IBM Intelligent Operations Center configuration, then remediation might not be required.
- Does the product vulnerability affect the operating system being used? Some vulnerabilities may only exist when running specific operating systems.

For each item on a checklist, these factors were analyzed to determine the action required for IBM Intelligent Operations Center. This analysis and remediation results in one of four assessments:

Not Applicable (NA)
The affected product or configuration is not part of the IBM Intelligent Operations Center environment.

Not a Finding (NF)
The installed version and fix level of the product is not affected, or the

product is not used in a way that exposes the vulnerability. This assessment is also used if the configuration does not expose the vulnerability.

Open The vulnerability applies to the installed product version and fix level, however, no remediation is available for the product. This assessment is also used if the system is configured in a way that exposes the vulnerability. For example, allowing world-write permissions on a directory because a product requires it.. This assessment is also used when applying a remediation might depend on organization policies such as password policies on length or character mix.

Fixed A remediation of an open vulnerability was applied and verified.

Table 1 shows an example analysis. The second example shows the handling of a product not installed on any IBM Intelligent Operations Center server.

Table 1. Example vulnerability assessments

ID	Name	Severity	Application server	Event server	Data server	Management server	Explanation
2011-B-0082	Multiple Vulnerabilities in IBM Websphere Application Server	I	NF	Open	NA	NF	Affects version prior to 6.1.0.39 and 7.0.0.19
2011-B-0085	Multiple Denial of Service Vulnerabilities in Wireshark	I	NA	NA	NA	NA	Wireshark not installed

Checklist selection

The checklists used for each server are based on the software installed on that server. Specific checklists address vulnerabilities for product types, for example, databases. Others address issues with specific products within a category, for example, DB2®.

Not all product types have specific checklists. Generic vulnerabilities are documented in the Application Security checklist or in an operating system-related list.

The following types of checklists are used by cyber hygiene:

Application security
Lists system level vulnerabilities. Some relate to the software development and testing practices and others address application-specific vulnerabilities such as not using encrypted passwords during user authentication.

Unix/Linux
Lists vulnerabilities related to configuration, password management, file system partitioning, and so on.

Web Server
Lists vulnerabilities related to HTTP servers.

Database
Lists vulnerabilities related to database servers.

Directory Servers
Lists vulnerabilities related to LDAP servers.

Enterprise System Management
Lists vulnerabilities related to enterprise system management tooling and system management processes.

Network security is not addressed by the checklists since network security configuration must be determined by a customer's policies and network architecture. Network security configuration must be handled according to the needs of each installation.

Cyber hygiene default configuration

The cyber hygiene feature sets Linux default configurations and policies to more secure options than are set in the default operating system installation. These default settings can easily be modified by system administrators to conform with the security policies for the installation.

An enterprise's IT operations administrative group is responsible for the security of their systems. This includes managing network access and internal security policies and processes.

Where the cyber hygiene default settings are inconsistent with enterprise policy, enterprise policies must take precedence. Remember that local security policy settings have not been tested for their impact on system functionality. The same care taken when applying security policy to products not deployed with cyber hygiene should be taken when applying security policy to IBM Intelligent Operations Center.

While IBM Intelligent Operations Center cannot be automatically be configured for individual enterprise security policies, IBM Intelligent Operations Center can be configured to remove known vulnerabilities. Cyber hygiene configures IBM Intelligent Operations Center with a set of default, best practice policies creating a foundation for system administrators to use when applying specific organizational policies and practices

Remote login by root user

Cyber hygiene disables IBM Intelligent Operations Center server log on by the **ssh** command as the `root` user. All other remote access services, including the **telnet** and **rsh** commands, are disabled.

Remote log on using the `root` account is a security risk because the `root` account can be used in a remote attack. The identity of the person logging on as the `root` user is hidden. Someone compromising the system by accessing the `root` account can do so by the following methods:

- Accessing the `root` account directly:
  - By the `root` account having a password that has not been changed or can be easily guessed.
  - By direct `root` log on through a network.
  - By direct `root` log on using a privileged terminal.
  - By accessing single-user mode (runlevel 1) when not configured with password protection.
  - By a system defaulting authentication to a `root` log on.
- Accessing the `root` account indirectly:
  - By compromising a server already running as the `root` account.
  - By creating or deploying malware that will run with `root` privileges.

While there are many ways these attacks can be implemented, most all rely on the following configuration weaknesses:

- Weak passwords and weak password management.
- Weak network security.
- Weak system access control.
- Weak configuration management. For example, not enforcing the principle of least privilege where access is only granted to needed resources.

A best practice is to allow users to log on with a non-privileged account and then use the **su** command to change to a privileged account. The **su** command will generate an audit event indicating the user logging on as a privileged user.

Note: If IBM Intelligent Operations Center is installed on a system where no users are defined with remote log on authority, system administrators might not be able to log on to the servers after cyber hygiene is run. In this case an administrator would need to physically access the server, or use the hypervisor virtual console, to log on and create an ID for remote log on.

Cyber hygiene disables remote `root` user log on by making the following changes on each IBM Intelligent Operations Center server:

- The `/etc/securetty` file is changed so only the `console` entry is included. This allows direct terminal log on from the system console only.
- The **PermitRootLogin** parameter in the `/etc/ssh/sshd_config` is set to `"no"`.
- A GRUB password is set by the installation.
- Some PAM authentication modules are modified to remove excessively permissive rules, such as access to the console, enabling **rhost** access under an account, and so on.
- Permissions for the **cron** and **at** commands are restricted.
- Strong access permissions are set for the `root` home directory.
- All IBM Intelligent Operations Center servers are configured to run on an ID other than `root` except for daemons providing services to servers and cannot be accessed by users.

Note: Cyber hygiene does not modify the `/etc/sudoers` file.

Related concepts:

"Other changes" on page 11
Cyber hygiene makes other changes to address security exposures.

Related reference:

Chapter 3, "Processes running under the `root` account," on page 13
After cyber hygiene is run, some processes still must run under the `root` account.

Default password management policies

Cyber hygiene configures the default Linux operating system password management policies.

The default password management policies set by cyber hygiene are shown in Table 2.

Table 2. Default cyber hygiene password management policies

Policy	Value or setting
Minimum password length	8 characters

Table 2. Default cyber hygiene password management policies (continued)

Policy	Value or setting
Accepted characters	uppercase letters, lowercase letters, numbers, special characters (: ; ! ` ~ @ # $ % ^ & * ( ) - _ = + [{] } \ | ' " , < . > / ? and the space character)
Content rules	none
Number of failed log on attempts before locking out user	3
Minimum time between password changes	1 day
Maximum time between password changes	60 days
Are passwords required on accounts?	yes
When can a password be reused?	after 5 different passwords
Log in required after inactivity	15 minutes of inactivity
Delay between log on failures	4 seconds

The `/etc/pam.d/system-auth` and `/etc/login.defs` files are modified when setting the cyber hygiene default policies.

These settings are intended to be the minimum necessary for reasonable security practices. You should modify these settings to match your organization's security policies. Some areas where you might want to change the default settings are as follows:

- While the default configuration sets the minimum password length to 8 characters, best practices for secure systems generally considers secure passwords to be 14 or more characters in length.
- The maximum time between password changes should be set to a value appropriate for your organization. This is defined in the **`inactive`** parameter in the `/etc/shadow` file. At the defined point in time the user is forced to change the password at log on. If the user fails to change the password, the password must be reset by a privileged user. Whether the value specified in the `/etc/shadow` file is used depends on the default action specified in the `/etc/default/useradd` file. If the `/etc/default/useradd` file specifies -1, the password does not expire. If `/etc/default/useradd` specifies 0, the account is locked. If any other value in the `/etc/default/useradd` file is defined, the **`inactive`** parameter value in the `/etc/shadow` is used for the password expiration.
- Rules concerning the complexity and content of passwords should be addressed and implemented according to the enterprise security policy.

See the Linux documentation for more information on managing password policies.

Disabled Linux services

Cyber hygiene disables or uninstalls vulnerable Linux services. These services can allow system access and should only be started or installed if there is a need for them.

The following Linux services (daemons) are not started by default. They can be started if needed.

- inetd/xinetd
- portmap
- avahi-daemon
- bluetooth
- cups
- hidd
- isdn
- rhnsd
- canna
- pcmcia
- ypbind
- autofs
- smartd
- netfs
- snmpd
- nfs
- samba

These services can be started using the **service** *service_name* **start** command.

Note: These services, if not properly configured, can be compromised and allow unauthorized access to the system. This is why, for system security, they are not started by default.

The following Linux services are removed. They can be reinstalled if needed using the **rpm** or **yum** commands. For example, the **yum install httpd** command will install the HTTP daemon package.

- tcpdump
- sendmail
- squid
- vnc-server
- httpd
- mod_python
- mod_perl
- mod_ssl
- webalizer
- httpd-manual

Note: These services are removed from Linux because they have a high potential for causing security exposures in server environments.

Removed user IDs

A standard Linux installation contains a number of user IDs that are not desirable in a secure production environment. Cyber hygiene removes these user IDs from the Linux user registry and `/etc/passwd` file. The associated home directories are also removed.

The following user IDs are deleted and can be recreated if needed.

- games

- news
- ftp
- halt
- shutdown
- reboot
- who
- gopher
- lp
- rpcuser
- uucp

If these user IDs are required, standard Linux administration procedures can be used to create them.

Audit rules

Standard auditing in Linux is minimal since audit files can quickly grow. However, when security is an issue, additional auditing is critical to be able to determine what happened in an incident. Cyber hygiene scripts add a set of additional audit rules for all Linux run levels. Events matching these rules will be logged into the standard system log files.

The following Linux audit rules are added and can be modified if needed.

- Failed attempts to access programs and files
- Deletion of programs and files
- Administrative, security, and privileged actions
- Access control permission changes

Having good audit logs is a good security practice. If for some reason the auditing defined by cyber hygiene needs to be changed, the `/etc/audit/auditd.conf` and `/etc/audit/audit.rules` files need to be modified. Cyber hygiene turns on auditing for all five runtime levels of Red Hat Enterprise Linux.

File and directory permissions

Cyber hygiene changes existing file and directory permissions to meet security best practices.

The file and directory permission changes made by cyber hygiene are as follows:

Restriction of system scripts

Sensitive security system scripts cannot be accessed by users without the appropriate privileges.

Removal of world-write permission

Users cannot write to directories that are not public. Applications and users needing to modify files and directories must be the owner, or a member of the group, for the file or directory.

Removal of world-read and execute permission

The world-readable and world-executable permissions are removed for many files and directories. In particular, these permissions are removed from user home directories. Applications and users needing to read or run files must be the owner, or member of the group, for the file or directory.

Other changes

Cyber hygiene makes other changes to address security exposures.

Batch programs - `at` command

To stop non-privileged users from using the **at** command to run batch programs at a particular time, cyber hygiene deletes the `at.deny` file and creates an empty `at.allow` file.

The `at.allow` file defines the users allowed to run the **at** command. An `at.allow` file containing no user IDs implies that no users, other than privileged system IDs, can run the **at** command. If the `at.deny` file, which defines users explicitly not allowed to use the **at** command, exists, but the `at.allow` file does not exist, then all users, except those in the `at.deny` file, are allowed to run the **at** command. If neither file exists, only the superuser can run the **at** command.

By default Red Hat Enterprise Linux is configured to allow users to execute the **at** command.

Batch programs - `cron` command

Users without administrative privileges are not allowed to run the **cron** command to schedule batch programs.

Ctrl-Alt-Del

The Ctrl-Alt-Del key combination is disabled so it cannot be used to shut down the system.

Related concepts:

"Remote login by root user" on page 6
Cyber hygiene disables IBM Intelligent Operations Center server log on by the **ssh** command as the `root` user. All other remote access services, including the **telnet** and **rsh** commands, are disabled.

Remediation tools

IBM Intelligent Operations Center cyber hygiene functionality provides remediation tools to correct vulnerabilities in the installed IBM Intelligent Operations Center system.

Remediation tools are run when cyber hygiene is run after IBM Intelligent Operations Center installation is complete. These tools can also be run when the system is in production to find and correct vulnerabilities that might be created when other products are installed on the servers or as a result of system use.

Vulnerability scanner

The scanner consists of scripts that review the IBM Intelligent Operations Center system and identify vulnerabilities. For example, the scanner identifies directories with write privileges for any user.

The scanner creates a findings file used by the remediation scripts. The findings file lists identified vulnerabilities within the IBM Intelligent Operations Center system.

The scanner scripts do not make changes to the IBM Intelligent Operations Center system. The scanner only identifies vulnerabilities. It can be used after remediation to validate the changes made by the remediation scripts.

Vulnerability remediation scripts

Cyber hygiene has three types of remediation scripts:

- Scripts that make configuration changes which do not require scanning, which can be easily reversed, or have no noticeable runtime impact on the system. For example, changing the default file access permission of the man pages to 644.
- A script to disable remote logon with the `root` account.
- A script that processes the findings file created by the scanner and resolves identified vulnerabilities.

  Care should be taken in using this script after additional products are installed. Some products require less strict settings and can malfunction after these scripts are run. Review the findings files created by the scanner scripts for potential risks before running any remediation scripts.

Remediation logs

Scanning and remediation scripts log their actions in four log files on each IBM Intelligent Operations Center server. These logs are located in the `/var/BA15/CH/results` directory. Subdirectories contain working copies of the scan and remediation results.

The scanner is run twice: once to remediate vulnerabilities and a second time to log remediations not done. The log from the second run can be used by the administrator to determine if manual remediation steps are required.

Chapter 3. Processes running under the root account

After cyber hygiene is run, some processes still must run under the root account.

Processes running under the root account can be vulnerable if a user or process can obtain root privileges through privilege escalation. Normally this is only a problem for services processing requests originated by a user. User-originated requests can contain maliciously configured input that can compromise the server. Services processing user requests are systems providing user interfaces or accessible application programming interfaces (APIs).

Linux daemons are not normally at risk since they usually only start, stop, or respond to well-defined system events. In many cases these daemons must run as the root account so they can control other processes or respond to critical system events. As long as a user-accessible server itself is not running as root, daemons running under the root account do not present as serious an exposure.

With the exception of Tivoli® Netcool/OMNIbus, all product servers in IBM Intelligent Operations Center are configured under IDs that do not have system privileges. Tivoli Netcool/OMNIbus provides monitoring and management services across all IBM Intelligent Operations Center hosts and servers.

Table 3 lists the processes that continue running as the root account after cyber hygiene is run.

Table 3. IBM Intelligent Operations Center environment processes running as root

Server	Product	Process Name	Explanation
data server and management server	DB2	db2wdog	This daemon process receives system events and propagate them to multiple child processes. The db2wdog process manages the db2sync processes and requires root level management.
data server and management server	DB2	db2chkpwd	This daemon authenticates the user ID and password of the user or application connecting to a database. The db2chkpwd process needs to read the /etc/shadow password file.
data server and management server	DB2	/opt/IBM/DB2/bin/db2fmcd	This daemon serves as a fault monitoring coordinator. It must run as root to monitor all DB2 instances.
data server and management server	DB2	/usr/sbin/rcst/bin/rmcd and /usr/sbin/rcst/bin/IBM.ConfigRMd	These commands manage the high availability solution for DB2. They need access to all databases on the servers configured for high availability.
event server	IBM Tivoli Monitoring agents for Lotus® Domino®	kgbagent, kgbclient, kslagent	These monitoring agents need to run as root to track Lotus Domino server activity.
application server, event server, and management server	IBM HTTP Server	httpd -d, http -f	Linux requires root access to listen on ports less than 1024. Standard HTTP ports are 80 through 443. IBM Intelligent Operations Center uses port 82. The httpd -d and http -f processes must run as root. Any alternate configuration is the responsibility of the installation as part of comprehensive network and security policy and configuration.

© Copyright IBM Corp. 2011, 2012

Table 3. IBM Intelligent Operations Center environment processes running as `root` (continued)

Server	Product	Process Name	Explanation
data server	IBM Tivoli Monitoring agents	`klzagent`, `kcawd`	These are monitoring and management agent processes. These processes monitor operating system and application processes and resources.
application server	IBM Tivoli Monitoring agents	`klzagent`, `kcawd`, `khtagent`, `kynagent`	These are monitoring and management agent processes. These processes monitor operating system and application processes and resources.
event server	IBM Tivoli Monitoring agents	`klzagent`, `kcawd`, `khtagent`, `kynagent`, `kmcrca`, `kgbagent`, `kgbstart.sh`, `kgbclient`, `kslagent`, `kmqagent`, `/opt/IBM/ITM/JRE/lx8266/bin/java`	These are monitoring and management agent processes. These processes monitor operating system and application processes and resources.
management server	IBM Tivoli Monitoring agents	`cms`, `kdsmain`, `KfwServices`, `klzagent`, `kcawd`, `kynagent`, `/opt/IBM/ITM/li6263/iw/java/jre/bin/java`, `/opt/IBM/ITM/li6263/iw/java/bin/java`	These are monitoring and management agent processes. These processes monitor operating system and application processes and resources.
event server	Tivoli Netcool/OMNIbus	`/usr/ibm/common/acsi/jre/bin/java`, `/opt/IBM/netcool/omnibus/platform/linux2x26/bin/nco_pad`	The `nco_pad` process is the process agent daemon that monitors all the process agents. The daemon requires access to system resources. The process agent daemon does not present a user interface. It only manages other processes.

Related concepts:

"Remote login by root user" on page 6
Cyber hygiene disables IBM Intelligent Operations Center server log on by the **ssh** command as the `root` user. All other remote access services, including the **telnet** and **rsh** commands, are disabled.

Chapter 4. Cyber hygiene exceptions

Once cyber hygiene is run, there remain known exceptions to the preferred security configuration.

An ideal configuration would not have exceptions to best practice settings. However, most systems have exceptions. These exceptions do not present a significant risk, but might be problematic if not understood. For example, some programs might have to run with the **suid** bit set.

Security administrators need to understand the exceptions so they can verify if their system has been compromised. When scanning the system administrators can understand intended exceptions as opposed to malware.

Table 4. Cyber hygiene exceptions to the preferred security configuration

Vulnerability	Server	Instance	Explanation
GEN000360: GID set to value in the system range for Linux (0-499).	data server	`dasadm1`	The `dasadm1` Group ID (GID) is set to 102. This is the administration group for the DB2 runtime instance IDs. This group is automatically created when DB2 is installed.

© Copyright IBM Corp. 2011, 2012

Chapter 5. File permissions requiring system administrator evaluation

Cyber hygiene does not make changes for exposures in all file permissions and ownership. Some of these must be evaluated and remediated by system administrators since automated changes could make some system functions inoperable.

The cyber hygiene scripts log information on potentially affected resources. System administrators can review these findings and make appropriate system changes.

Findings files are located in the `/var/BA15/CH/results` directory on each IBM Intelligent Operations Center server. The file name is `scanrem-combined-log-`*`date-time`*`.log`. The timestamp indicates when cyber hygiene was run.

Table 5 lists vulnerabilities and recommended actions requiring review.

Table 5. Vulnerabilities requiring evaluation by the system administrator

STIGID	Description	Severity	Recommendation
GEN001220	Files, applications, and directories in system directories must be owned by a system account or an application account.	II	Review the ownership of the resource and manually change or document as required.
GEN001240	Files, applications, and directories in system directories must be owned by a system group or an application group.	II	Review the group ownership of the resource and manually change or document as required.
GEN001500	The home directory, listed for a user in the `/etc/password` file, should be owned by a user.	II	Review the ownership of the home directory and manually change the ownership, or document why it cannot be changed.
GEN001520	The home directory, listed for a user in the `/etc/password` file, should be owned by the user's primary group.	II	Review the group ownership of the home directory and manually change the group ownership, or document why it cannot be changed.
GEN001560	Files in the home directory, other than start up files, should have permissions no greater than 750.	III	Change permissions if exceptions are not already documented.
GEN002520	Public directories must be owned by the `root` account or an application user ID.	II	Review ownership and assign as appropriate.
GEN002540	Public directories must be owned by the `root`, `sys`, `bin`, or an application group.	II	Review group ownership and assign as appropriate.

© Copyright IBM Corp. 2011, 2012

Chapter 6. Product and component security certifications

Some of the products and components included as part of the IBM Intelligent Operations Center solution have security certifications.

Table 6. Security certifications of products installed with IBM Intelligent Operations Center

	Common criteria		FIPS 140-2		
Product	**Release**	**Level**	**Release**	**Certified?**	**IPV6**
IBM WebSphere® Business Monitor	None	None	7.5	Yes	Yes
IBM Cognos® Business Intelligence	10.1.1	None	None	None	Yes
DB2 Enterprise Server Edition with DB2 Spatial Extender	9.7	EAL4+ALC_FLR.1	9.1 FP2	Yes	Yes
IBM HTTP Server	7.0.0.19		7.0	Yes	Yes
Lotus Domino	None	None	8.0.1	Yes	Yes
Lotus Sametime® Standard	None	None	8.5	Yes	Yes
Tivoli Access Manager for e-Business	6.0 FP3	EAL3+ALC_FLR.1	6.0	Yes	Yes
Tivoli Composite Application Manager	None	None	None	None	Yes
Tivoli Directory Integrator	None	None	7.0	Yes	Yes
Tivoli Directory Server	6.2	EAL4+ALC_FLR.1	6.1	Yes	Yes
Tivoli Identity Manager	5.0	EAL3+ALC_FLR.1	None	None	Yes
Tivoli Monitoring	None	None	6.2.0.1	Yes	Yes
Tivoli Netcool/Impact	None	None	5.1	Yes	Yes
Tivoli Netcool/OMNIbus and XML probe	7.1	EAL2	All	Yes	Yes
Tivoli Service Request Manager®	None	None	All	Yes	Yes
WebSphere Application Server Network Deployment	6.1.0.2	EAL4+ALC_FLR.1	All	Yes	Yes
WebSphere Application Server for Tivoli Service Request Manager	6.1.0.2	EAL4+ALC_FLR.1	All	Yes	Yes
WebSphere Message Broker	6.0.0.3	EAL4+ALC_FLR.2 (de)	6.1	Yes	Yes
WebSphere MQ	6.0.1.1.	EAL4+ALC_FLR.2	All	Yes	Yes
WebSphere Operational Decision Manager (Rules Engine)	None	None	None	None	Yes
WebSphere Portal Enable	5.0	EAL2	All	Yes	Yes

Products with FIP 104-2 certification is normally due to the use of IBM Crypto for C and Java modules. The certificate numbers for these products are shown in Table 7.

Table 7. FIPS 140-2 certificates

Module	**Certificate number**
IBM Crypto for C (V8.0.0)	1433

© Copyright IBM Corp. 2011, 2012

Table 7. FIPS 140-2 certificates (continued)

Module	Certificate number
IBM CryptoLite for Java (V4.2)	910
IBM CryptoLite for C (V4.5)	899
IBM Java JCE 140-2 Cryptographic Module	497
IBM Java JSSE FIPS 140-2 Cryptographic Module	409
IBM SSL Lite for Java	406

Related information:

Common Criteria: http://www.commoncriteriaportal.org/

Security Evaluations for IBM Products

Chapter 7. Products and components included with IBM Intelligent Operations Center

The IBM Intelligent Operations Center solution installs a number of software products and components.

The software products and components and the servers they are installed on are shown in Table 8.

Table 8. Products installed with IBM Intelligent Operations Center

Product	Application server	Data server	Event server	Management server
IBM WebSphere Business Monitor 7.5	installed	not installed	not installed	not installed
IBM Cognos Business Intelligence 10.1.1	installed	not installed	not installed	not installed
DB2 Enterprise Server Edition with DB2 Spatial Extender 9.7.0.5	not installed	installed	not installed	installed
Semantic model services	not installed	not installed	not installed	installed
IBM ILOG® CPLEX® Optimization Studio 12.4	installed	not installed	not installed	not installed
Jazz Foundation Server (for Semantic model services) 3.0.1	not installed	not installed	not installed	installed
Lotus Domino 8.5.3.1	not installed	not installed	installed	not installed
Lotus Sametime Standard 8.5.2 + IFR1	not installed	not installed	installed	not installed
Tivoli Access Manager for e-Business 6.1.1.4	not installed	not installed	not installed	installed
Tivoli Composite Application Manager 7.1	not installed	not installed	not installed	installed
Tivoli Directory Integrator 7.1.0.5	not installed	not installed	not installed	installed
Tivoli Directory Server 6.3.0.8	not installed	installed	not installed	not installed
Tivoli Identity Manager 5.1	not installed	not installed	not installed	installed

© Copyright IBM Corp. 2011, 2012

Table 8. Products installed with IBM Intelligent Operations Center (continued)

Product	Application server	Data server	Event server	Management server
Tivoli Monitoring 6.2.2.1	not installed	not installed	not installed	installed
Tivoli Netcool/Impact 5.1.1.1 + IF003	not installed	not installed	installed	not installed
Tivoli Netcool/ OMNIbus 7.3.1.2 and XML probe	not installed	not installed	installed	not installed
Tivoli Service Request Manager 7.2.1.2	not installed	not installed	installed	not installed
WebSphere Application Server 1.1.0.0 Feature Pack for Web 2.0 and Mobile	installed	not installed	not installed	not installed
WebSphere Application Server Network Deployment 7.0.0.21	installed	not installed	not installed	installed
WebSphere Application Server 6.1.0.29 for Tivoli Service Request Manager	not installed	not installed	installed	not installed
WebSphere Message Broker 8.0	not installed	not installed	installed	not installed
WebSphere MQ 7.0.1.7	not installed	not installed	installed	not installed
WebSphere Operational Decision Manager 7.5.1 (Rules Engine)	installed	not installed	not installed	not installed
WebSphere Portal Enable 7.0.0.2	installed	not installed	not installed	not installed

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

© Copyright IBM Corp. 2011, 2012

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, WebSphere, DB2, Rational®, Tivoli, ibm.com®, Passport Advantage®, Sametime, and Redbooks® are trademarks of the IBM Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Pentium is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Oracle, Javascript, and Java™ are registered trademarks of Oracle and/or its affiliates.

ArcGIS, EDN, StreetMap, @esri.com, and www.esri.com are trademarks, registered trademarks, or service marks of Esri in the United States, the European Community, or certain other jurisdictions.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Readers' Comments — We'd Like to Hear from You

IBM Intelligent Operations Center
IBM Intelligent Operations Center
Cyber Hygiene Overview
Version 1 Release 5

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 1-800-227-5088 (US and Canada)

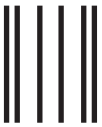
If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape



NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM
Information Development Department DLUA
P.O. Box 12195
Research Triangle Park, NC
USA 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in USA