Best Practices for BladeCenter Security

As you evaluate the security requirements of your BladeCenter® environment, be sure to consider that unsecured systems-management tools can be used to damage hardware and software. It is extremely important that you understand all security risks in your system environment and what you can do to minimize these risks. The best security solution for your environment requires that you implement a combination of security features, administrative procedures, and other controls to achieve the level of security that your environment requires.

You are responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communications facilities. This document describes general methods that you can use to help secure your hardware.

Systems-management tools are potentially dangerous pieces of software, especially if they are used with malicious intent. Systems-management agents typically have access to the hardware and software of the managed system, and can cause serious problems if they are not secured properly. It is extremely important that you understand what security risks are present, what security capabilities exist, and how to plan for the safest and most efficient use of these features.

Note: The practices described in this document will not secure your environment completely. The purpose of this information is to help you achieve the best possible level of security using the capabilities of your hardware. This document includes links to additional information that can help you secure your environment completely.

For more information about the specific security features of your hardware, see the documentation for your blade server on the BladeCenter blade servers page in the BladeCenter Information Center, as well as the documentation resources listed in "Related documentation" on page 2 of this document.

Securing communication and authentication

Use the general security, authentication security, web interface, and command-line interface security considerations in this section to help secure network communication and authentication.

General security considerations

Be aware of the following security considerations:

- The physical security of your environment is important; limit access to rooms and racks where systems-management hardware is kept.
- Where possible and practical, place the systems-management hardware in a separate subnet. Typically, only administrators that Local Area Network (LAN) should have access to the systems-management hardware, and no basic users should be given access.
- Install a redundant advanced management module to provide access if the primary management module fails.
- Do not enable the external management ports of the BladeCenter Ethernet switch modules (ESMs). This will ensure that you separate the management traffic from the production LAN traffic. Instead, use the connection of the management module to the internal Ethernet interfaces of the ESMs.
- At a minimum, make sure that critical firmware updates are installed. After making any changes, back up the configuration of your advanced management module, service processor, and system firmware.
- Set an appropriate boot sequence for a system to help prevent unauthorized installation of software or removal of data using a USB or other drive attached to the system.

Authentication security considerations

The following information can help you control who can access your network and the data available on it. See the documentation that came with your hardware for instructions to implement these concepts.

- When you choose passwords, do not use expressions that are easy to guess, such as `password`, `ibm`, or the name of your company. Keep the passwords in a secure place and make sure that access to the passwords is restricted. Implement a password policy for your company.

  Important: Always change the default user name and password. Strong password rules should be required for users who are permitted to access. Only the users who are authorized to update firmware components should have firmware-update privileges.
- For each advanced management module and service processor, create a new supervisor user with a different ID and password, and delete the default user USERID.
- Data such as user IDs, passwords, and configuration files should be encrypted.
- Establish power-on passwords for users as a way to control who has access to the data and server setup program on the server.
- Use an unattended boot mode password to lock the system keyboard to all entries except for the password.
- Use the various authorization levels that are available for different users in your environment. Do not allow all users to work with the same supervisor user ID.
- Use secure Lightweight Directory Access Protocol (LDAP) to query and modify data of directory services. When an LDAP server is available, configure LDAP for user authentication. Define at least one supervisor user locally in case you have problems with LDAP.

Web interface considerations

Use the following information to help secure a web interface that you use to manage your system environment.

- To help secure the web interface of your advanced management module, use the Secure Sockets Layer (SSL) capability. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.
- Change the port of the HTTPS protocol.

Note: For more information about the preceding security measures, see the Configuring security topic on the BladeCenter Information Center website.

Command-line interface considerations

Use the following information to help secure a command-line interface (CLI) that you use to manage your system environment.

- Activate the Secure Shell (SSH) protocol, disable Telnet, and use SSH instead of Telnet.
- Use the **security** command to enable and display the state of the data encryption feature for sensitive information stored in the advanced management module, such as passwords and keys.

Note: For more information about the following security measures, see the Secure Shell (SSH) connection and security command topics on the BladeCenter Information Center website.

Related documentation

For more information about IBM® BladeCenter hardware and the advanced management module, see the following documentation resources:

BladeCenter Information Center
http://publib.boulder.ibm.com/infocenter/bladectr/documentation

Advanced management module
http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/adv_mgt_mod_product_page.html

For more information about systems-management security, see the following documentation resources:

IBM Security Solutions
http://www-03.ibm.com/security

Introducing the IBM Security Framework and IBM Security Blueprint
http://www.redbooks.ibm.com/abstracts/redp4528.html

IBM Institute for Advanced Security
http://www-304.ibm.com/industries/publicsector/us/en/rep/%21%21/xmlid=192485

IBM Security Technology Outlook
http://www-03.ibm.com/security/outlook.html

First Edition (February 2011)