IBM WEBSPHERE TRADITIONAL V9.X SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 1

23 August 2018

Developed by IBM and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

The IBM WebSphere Traditional V9.x Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. This document is meant for use in conjunction with other STIGs such as the Application Security and Development and appropriate Operating System (OS) STIGs.

WebSphere is a Java-based software framework and middleware that is designed to host Java-based web applications. The product provides software libraries that hosted applications can use as well as an operating environment for web-based applications. IBM currently offers WebSphere in different profiles, including the WebSphere Liberty and the WebSphere Traditional profiles. This STIG was written to be applied to the WebSphere Traditional profile version 9.0. The scope of the STIG is intended to address the management and security posture of the WebSphere product, not the applications hosted on the application server.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing

Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. CONCEPTS AND TERMINOLOGY CONVENTIONS

2.1 WebSphere Design and Structure

WebSphere consists of the following concepts and elements:

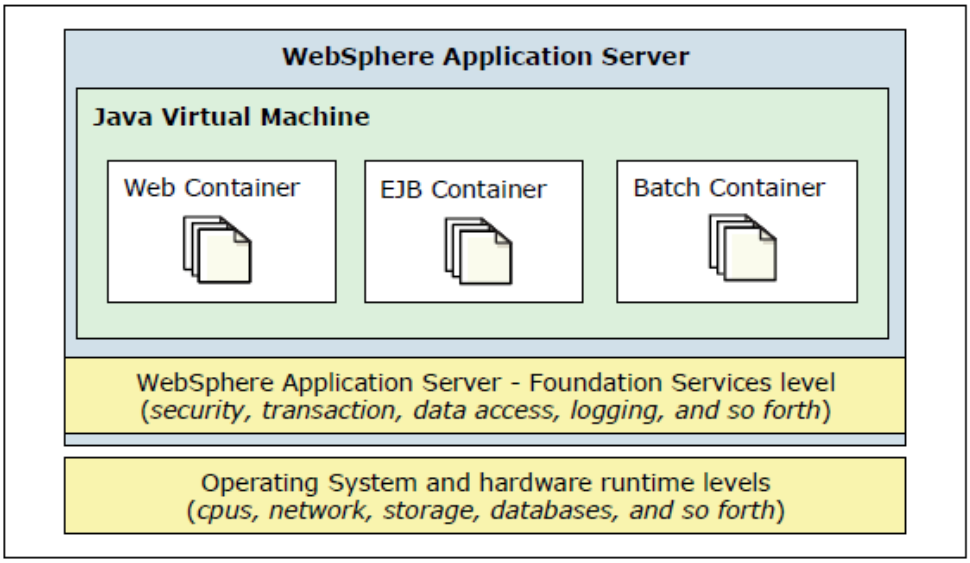
- Applications
- Containers
- Application servers
- Profiles
- Nodes, node agents, and node groups
- Cells
- Deployment manager

2.1.1 Applications

At the heart of the WebSphere is the ability to run applications, including the following types of applications:

- Java Platform, Enterprise Edition (EE) applications
- Portlet applications
- Session Initiation Protocol (SIP) applications
- OSGi applications
- Batch applications
- Business-level applications

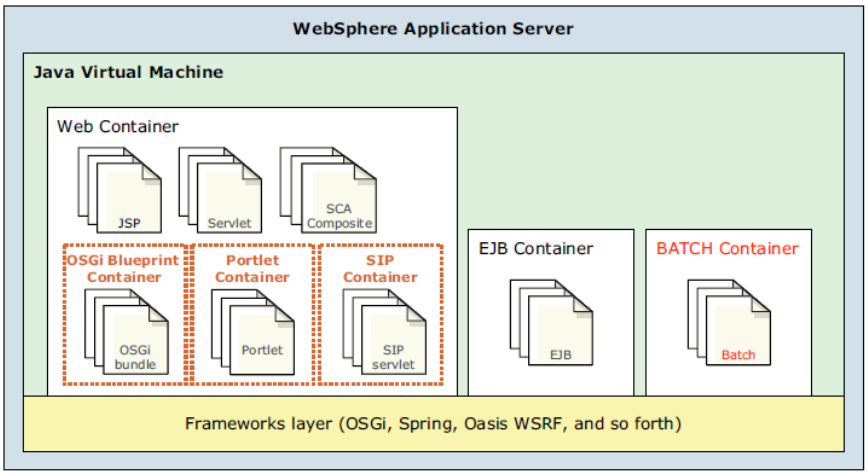
Figure 2-1: WebSphere Applications



2.1.2 Containers

- Containers provide runtime support for applications; they are specialized code in the application server that run specific types of applications.
- Containers can interact with other containers by sharing session management, security, and other attributes.

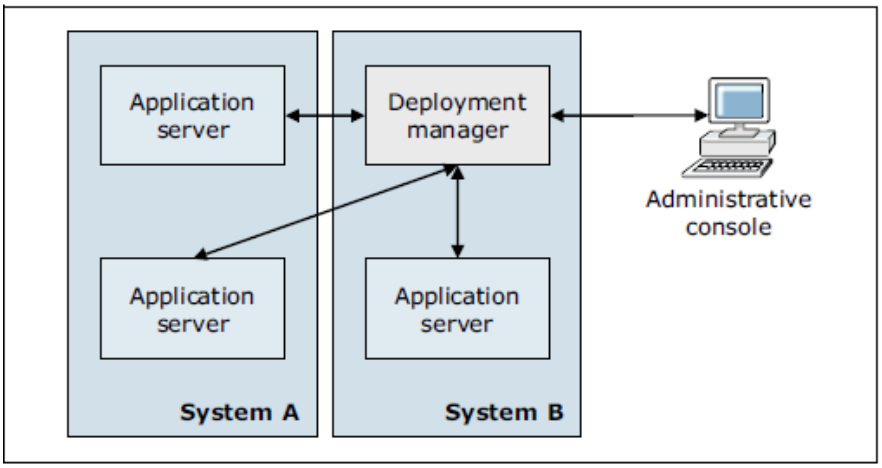
Figure 2-2: WebSphere Containers



2.1.3 Application Servers

- Standalone application servers
- Distributed application servers

Figure 2-3: Distributed Application Server Architecture

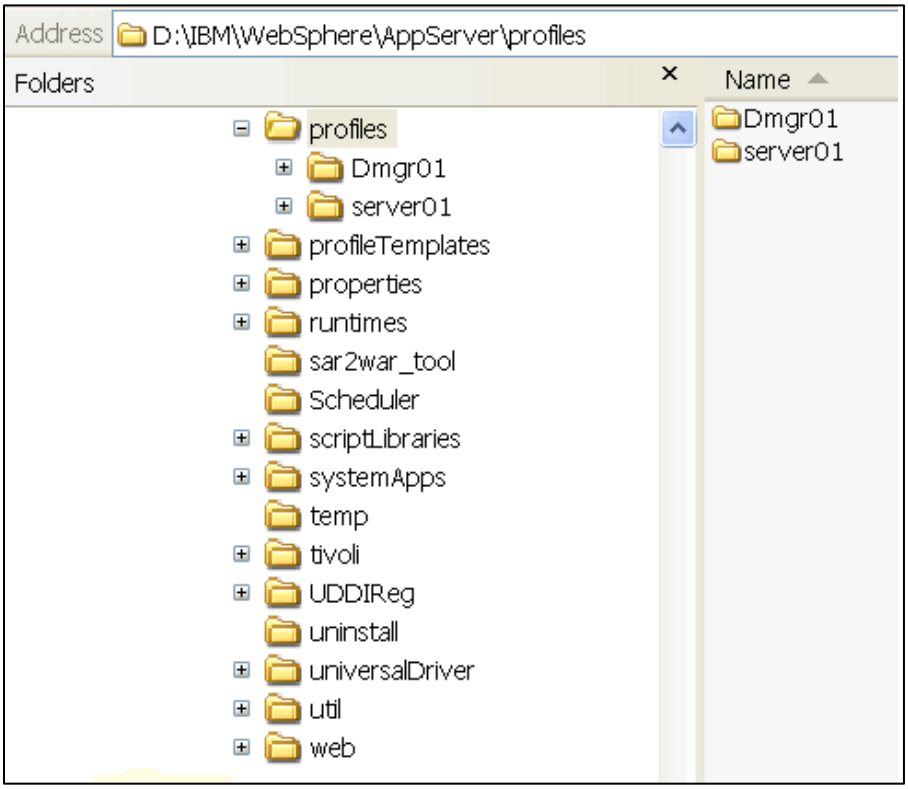


2.1.4 Profiles

- WebSphere Traditional runtime environments are built by creating sets of configuration files, named profiles. Do not confuse this terminology with the Liberty profile of WebSphere; they are not the same.
  - Each profile contains files that are specific to that run time (such as logs and configuration files).
  - Each profile is stored in a unique directory path selected by the administrator when the profile is created.

Note: You can create profiles during and after installation; after you create the profiles, you can perform further configuration and administration by using WebSphere administrative tools.

Figure 2-4: Profiles Directory Windows System

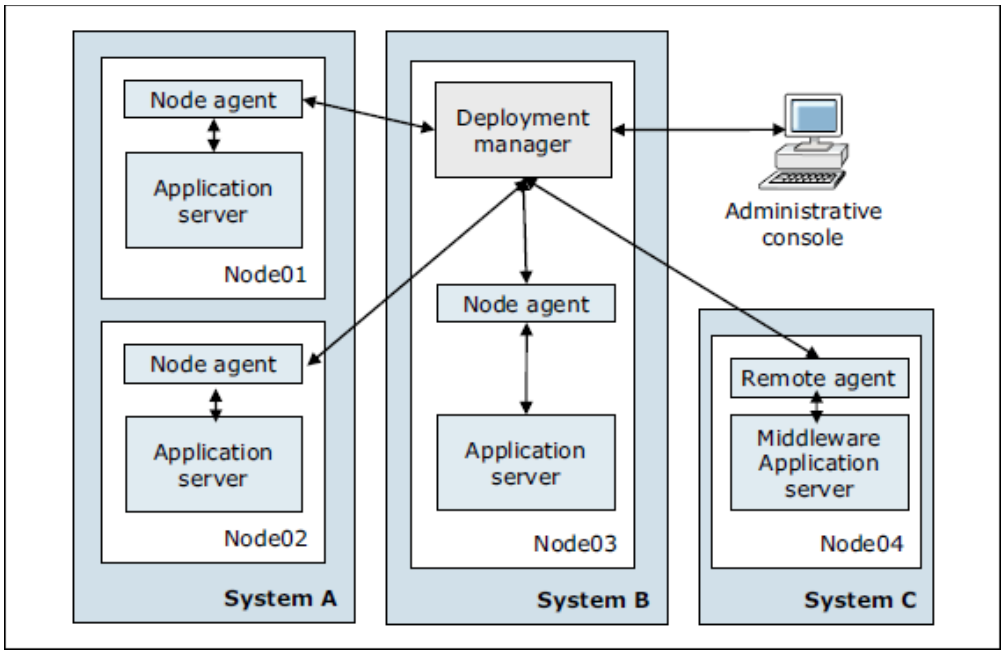


2.1.5 Nodes

- A node is an administrative grouping of application servers for configuration and operational management within one operating system instance.
- A stand-alone application server configuration has only one node.
- With Network Deployment, you can configure a distributed server environment that consists of multiple nodes that are managed from one central administration server.

Note: You can create multiple nodes inside one operating system instance, but a node cannot leave the operating system boundaries.

Figure 2-5: Node Concept



2.1.6 Cell

- A cell is a grouping of nodes into a single administrative domain.

2.1.7 Deployment Manager

- The deployment manager is the central administration point of a cell that consists of multiple nodes and node groups in a distributed server configuration; the STIG will often refer to the deployment manager as DMGR, which is a common practice when administering a WebSphere server.
- The deployment manager communicates with the node agents of the cell that it is administering to manage the application servers within the node.
- The deployment manager provides management capability for multiple federated nodes and can manage nodes that span multiple systems and operating systems; a node can be managed by a single deployment manager, and the node must be federated to the cell of that deployment manager.
- If the deployment manager is not available in the cell, the node agents and the application servers cannot synchronize configuration changes with the master repository; this limitation continues until the connection with deployment manager is reestablished.

Note: The configuration and application files for all nodes in the cell are centralized into the *master repository*. This centralized repository is managed by the deployment manager and regularly synchronized with local copies that are held on each of the nodes.

2.1.8 Web Servers

- Although web servers are independent products and are not within the scope of this STIG, technically they can be defined and managed by the administration processes of WebSphere Application Server; the STIG does not encourage or require that the third party web servers in the application architecture be managed by WebSphere.
- *Managed nodes* have a node agent on the web server system that allows the deployment manager to administer the web server.
- *Unmanaged nodes* are not managed by WebSphere Application Server.

2.1.9 Service Integration Bus

- The service integration bus (bus) is the communication infrastructure that provides service integration through messaging.

Figure 2-6: Service Integration Bus