Enterprise System Resiliency Guidelines

1. Introduction

This document is part of the series of Enterprise Technology Guideline (ETG) that establishes the official technology guidelines for achieving system resiliency and redundancy for all systems that provide business value to end users.

The guidelines provided in the following sections apply to all products and systems in VA, and they can be reviewed by product managers, IT planners, and developers. Links are provided for detailed implementation guidance that is used by engineering staff to design and implement solutions.

Each guide is independent and operates on different layers of application resiliency, redundancy, and accessibility. These guides fall into different areas-of-responsibility and may be supported by different teams.

2. Internal DNS Best Practices Guide

Executive Summary: The document "AS Internal DNS Best Practices Guide" provides best practices for configuring DNS settings on servers in the VA network. DNS configuration of the system hosting the application is usually found in the network settings or network adapter properties. Systems may have DNS automatically assigned and is preferred and acceptable. If the list needs to be configured manually, and that is done properly, it reduces risk, increases resolution speed, improves customer experience, and eases DNS troubleshooting.

Link to Document: Resiliency and Redundancy Design Patterns | CODE VA

3. CNS External DNS Guide

Executive Summary: The document "CNS External Guide DNS Guide" provides a process to initiate an externally available application or service into the Department of Veterans Affairs (VA) Enterprise begins with an Enterprise Security External Change Council (ESECC) request via *https://esecc.va.gov*. One of the resources available is a document that describes the various connections they support for review and approval. The document can be found under *Resources* > *Connections Defined*. Focusing on Domain Name Service (DNS) related connections through the Trusted Internet Connections (TICs) are the following connection types:

- Public Internet Service
- Business Partner Extranet (BPE)
- Domain Name Service – External

These are connection types that will generally have an external DNS component configured in the Trusted Internet Connections (TICs) as part of the standard configuration.

Link to Document: Resiliency and Redundancy Design Patterns | CODE VA

4. Domain Controller Best Practices Guide

Executive Summary: The document "AS_Domain Controller Best Practices Guide" outlines best practices for configuring domain controller settings on servers and applications in the VA network. Discovering domain controller to support an application's authentication and Lightweight Directory Access Protocol (LDAP) requirements starts in the Active Directory sites that supports the server hosing the application. The best practices of discovering the domain controllers are described in his document.

Link to Document: Resiliency and Redundancy Design Patterns | CODE VA

5. Application Load Balancer Guide

Executive Summary: The enclosed document "Application Load Balancer Guide" provides instruction on how to develop and deploy the right load balance technologies to meet availability requirements in the Department of Veterans Affairs (VA). Load balancing is one of the critical methods to provide fault-tolerant, highly available services. This is best practice for all systems and VA requires that the Critical-100 (C-100) systems must provide highly available services to fulfill the Office of Information Technology (OIT) and VA's mission.

Link to Document: Resiliency and Redundancy Design Patterns | CODE VA

Commented [TC1]: @Fang, Y The order of these guides needs to be as follows:
1.Internal DNS
2.External DNS
3.Domain Controller
4.Load Balancer

Document Version Control

Date	Version	Change Details	By
1/28/25	0.1	Original Draft	OCTO/AES
4/8/25	0.5	Updated Version	OCTO/AES
5/19/25	1.0	Final Version	OCTO/AES