IBM Security Secret Server
Version 10.4

Architecture and Sizing Guide

Contents

This document contains information for planning Secret Server architecture and resource allocation within your environment. Read through or use one of the following links to skip ahead to the relevant section.

Secret Server System Requirements

The following table describes the suggested software requirements for Secret Server. For more information, see System Requirements – Secret Server.

Requirement	Versions supported	Notes
Microsoft Operating System	Windows Server 2012 or newer	Windows Server 2008 R2 SP1 or newer is supported, but 2012 or newer is suggested. Small Business Server (SBS) is not supported. The Essentials edition is not supported.
Microsoft SQL Server	SQL Server 2012 or newer	*SQL Express Edition should not be used in production environments.
Microsoft Internet Information Services (IIS)	IIS 7 or newer	IIS needs to be added as a feature in the Windows Server. For information on adding IIS as a feature go here.
Microsoft .NET Framework	.NET Framework 4.6.1 or newer	Both 32-bit and 64-bit versions are supported. However, some features of Secret Server require 64-bit to operate.

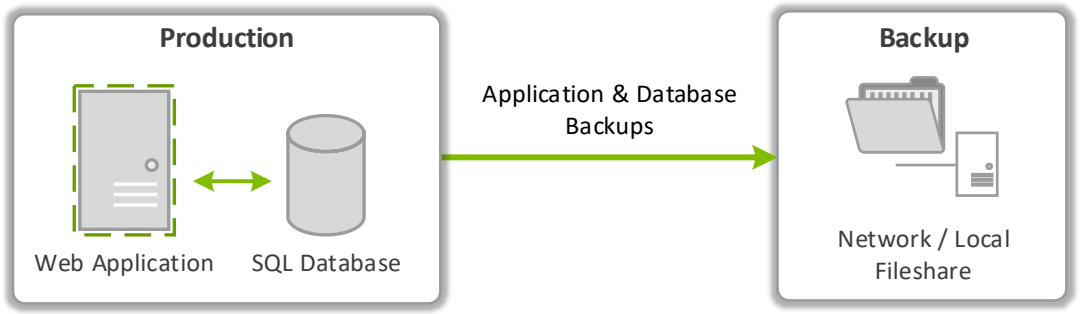
Secret Server Architecture

The following scenarios outline commonly deployed implementations of Secret Server. For more detailed information about Disaster Recovery options and configuring High Availability, see the Disaster Recovery guide.

Basic Configurations

Single Site, Single Server

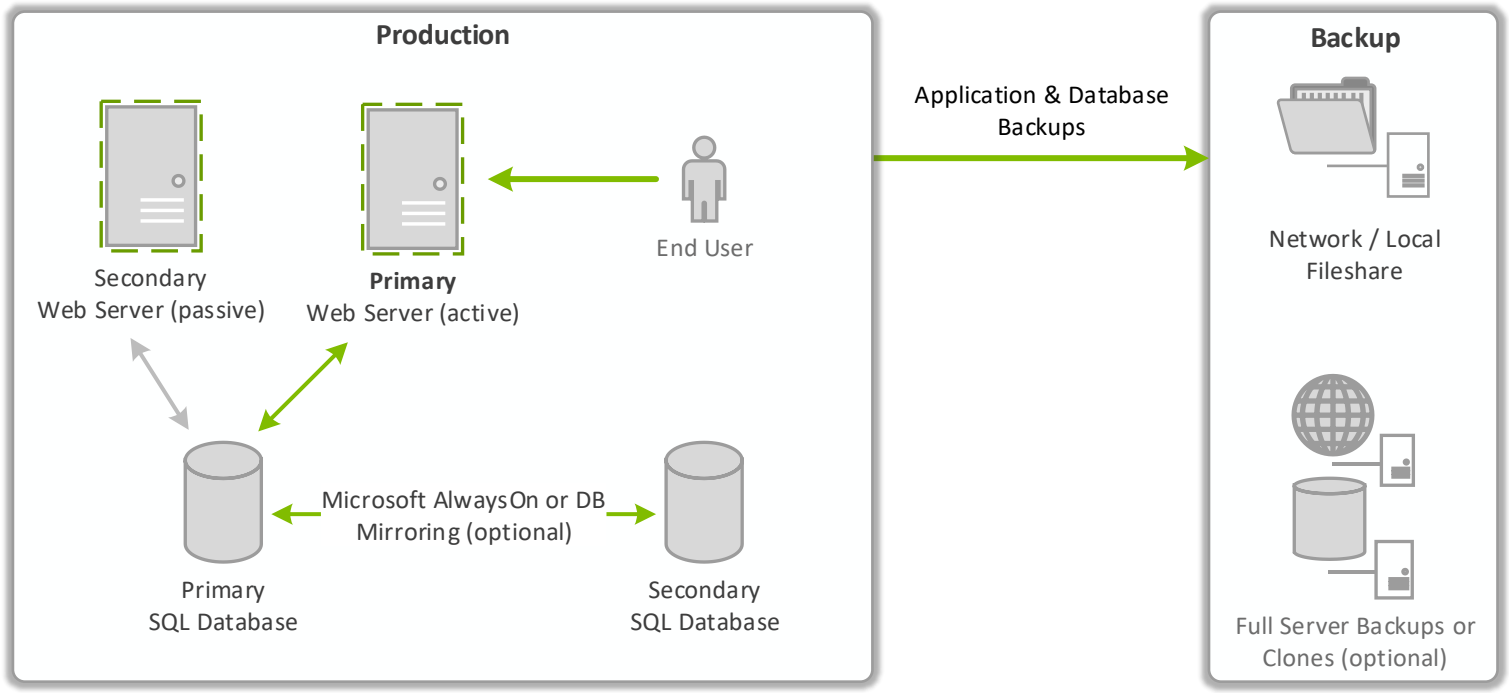
Suggested for: Secret Server Trials or Sandbox Environments, Secret Server Free, or Professional Edition



This diagram is an example of a basic Secret Server installation. You can install Secret Server and Microsoft SQL Server Express on a single Windows Server for trials or sandbox environments. However, the Express edition is not recommended for production environments due to RAM limitations. Automatic or manual application and database backup procedures can be used to stored backups on another server or file share. If the Windows Server is virtualized, using strategies such as making scheduled snapshots or having a hot/cold site might add more layers of redundancy.

Single Site, Active-Passive

Suggested for: Secret Server Professional or higher, SQL Standard Edition or higher required

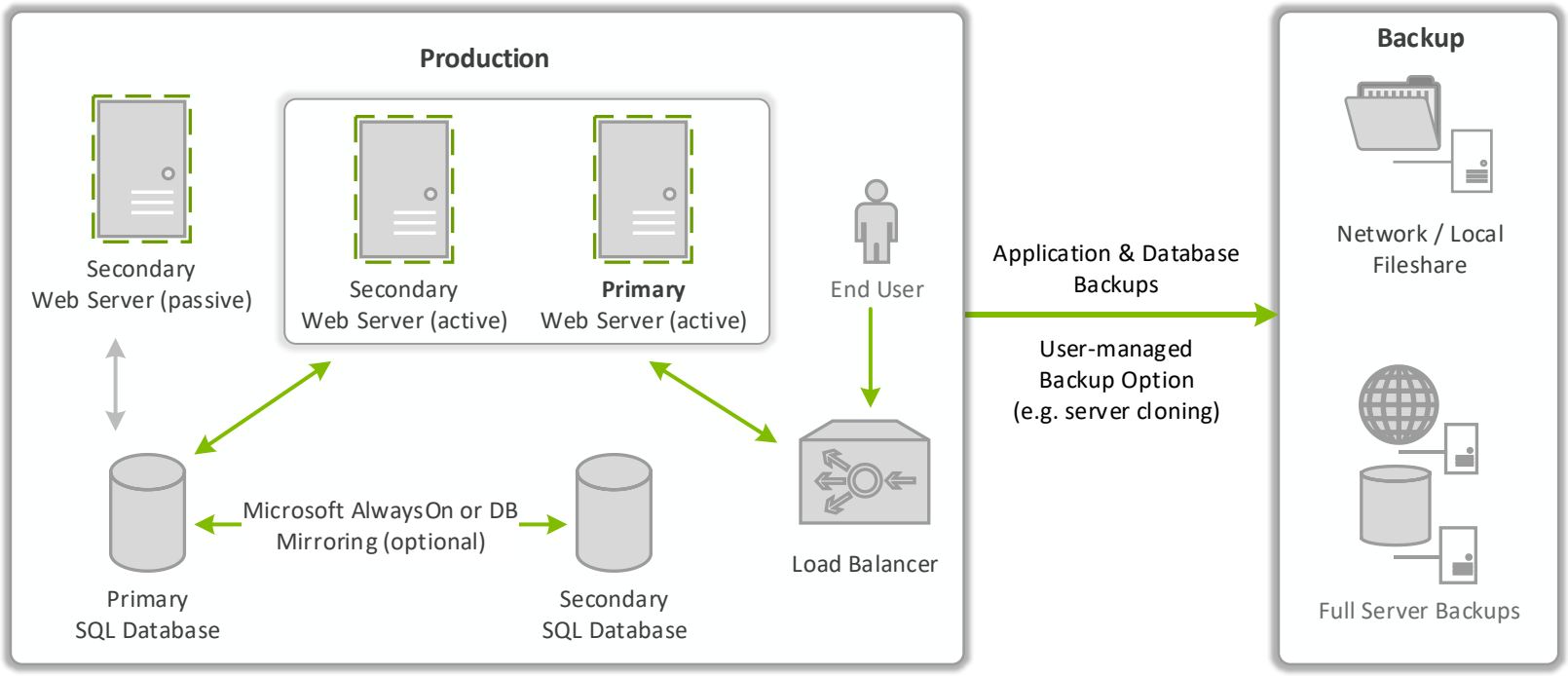


In this example, there are more than one front-end web servers, but only one active node. A web server node that is active means that users hit this site when you browse to Secret Server at any time. This server handles background processes (such as Remote Password Changing and Heartbeat) as well, making it the primary server in addition to the fact that it is active. The passive web server also points to the backend SQL database, but informs users that are browsing to it that they must use the active node to use Secret Server. If the active node is unavailable, the “Primary” status can be transferred to the passive node, and users can resume by using the application. You can have more than one passive server node (no limit), depending on the needs of your organization.

High Availability Configurations

Single Site, Active-Active

Suggested for: Secret Server High-Availability Add-On, SQL Standard Edition or higher required



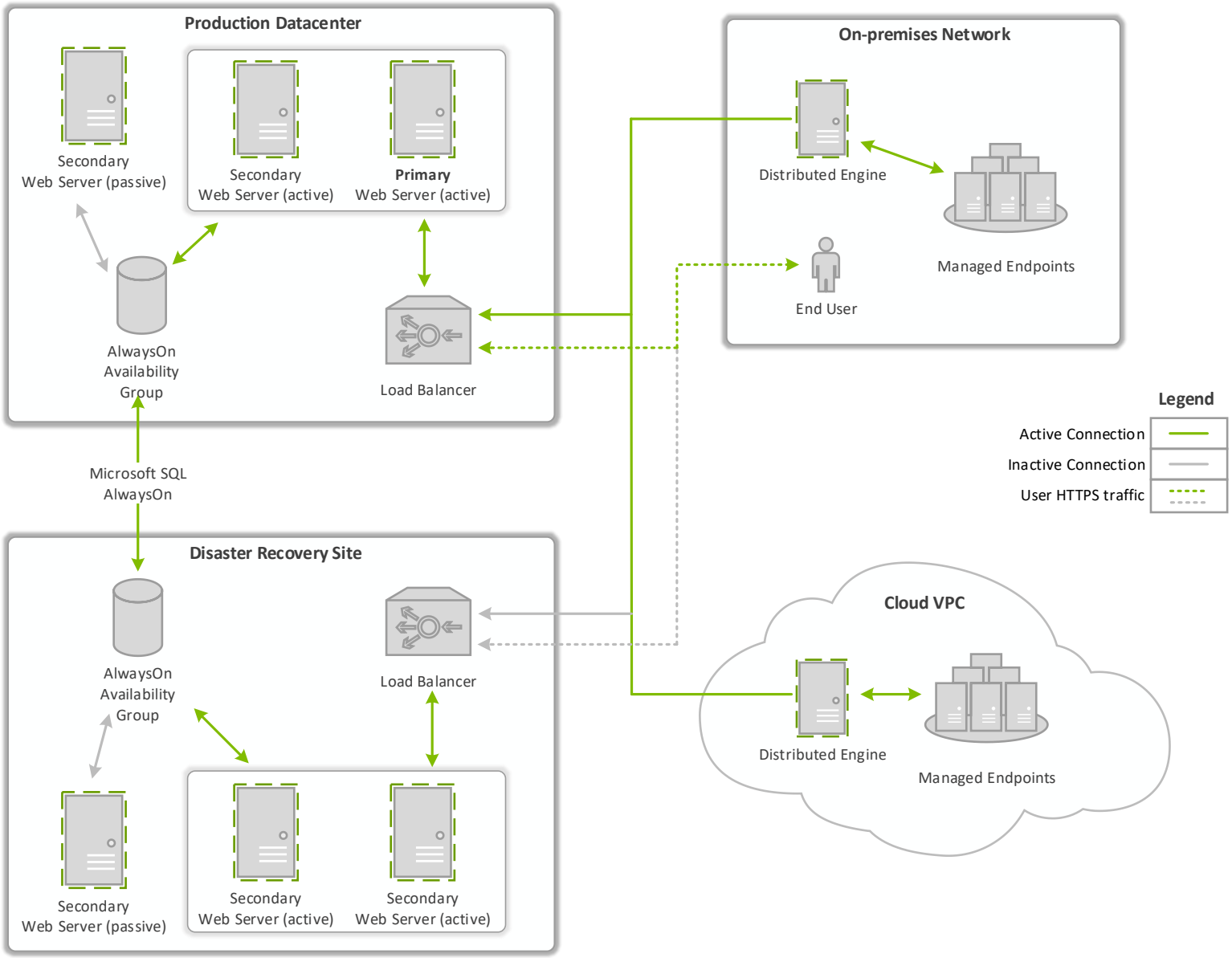
In this example, there are more than one front-end web servers, and more than one active node. Allowing users to use Secret Server through more than one active node simultaneously requires enabling clustering within the application. Only one server handles background processes (such as Remote Password Changing and Heartbeat). In this scenario, one of the active nodes are designated as the Primary server at any time. This designation is changed manually, if necessary, in the application. If the primary active node becomes unavailable, the “Primary” status is transferred to one of the other active nodes and users can continue by using the application without interruption. You can have more than one active and passive server nodes (no limit), depending on the needs of the organization.

Multi-Site, Active-Active

Suggested for: Secret Server Premium Edition, SQL Enterprise Edition

This deployment is an example of an implementation that a larger enterprise can use. You have more than one front-end web server, active node, and SQL AlwaysOn in use. A setup with this similar configuration exists in two sites. You can browse to the application through one load balancer at the production site. If anything happens on the production site that cannot be handled by the Active-Active setup at that location, administrators can direct users to the load balancer at the second site and an active server node there becomes primary. However, only one server handles background processes. It is suggested to offload Remote Password Changing, Heartbeat, Discovery, and so on, to Distributed Engines. This means that regardless of which server is Primary, Distributed Engines can retrieve workload tasks from Secret Server and connect to managed endpoints per usual.

The diagram for this configuration is on the next page.


Production Datacenter
Secondary
Web Server (passive)
Secondary
Web Server (active)
Primary
Web Server (active)
AlwaysOn
Availability
Group
Load Balancer
On-premises Network
Distributed Engine
Managed Endpoints
End User
Legend
Active Connection
Inactive Connection
User HTTPS traffic
Microsoft SQL
AlwaysOn
Disaster Recovery Site
AlwaysOn
Availability
Group
Load Balancer
Secondary
Web Server (passive)
Secondary
Web Server (active)
Secondary
Web Server (active)
Cloud VPC
Distributed Engine
Managed Endpoints

Secret Server Sizing

Hardware Requirements

For an installation of Secret Server that handles core tasks such as Remote Password Changing and Heartbeat:

Minimum Requirements

Web Server	Database Server
2 CPU Cores	2 CPU Cores
4 GB RAM	4 GB RAM
25 GB Disk Space	50 GB Disk Space

Suggested Requirements

Web Server	Database Server
4 CPU Cores	4 CPU Cores
16 GB RAM	16 GB RAM
25 GB Disk Space	100+ GB Disk Space

**Environments budgeting for over 10,000 Secrets are suggested to schedule a scoping call with an IBM engineer.*

To improve performance in larger environments where the **Discovery** or **Session Recording** features are used heavily, it is also suggested to scale up resources. If you are running Discovery or Session Recording:

Advanced Feature Requirements

Web Server	Database Server
8 CPU Cores	8 CPU Cores
16 GB RAM	16 GB RAM
25 GB Disk Space	100+ GB Disk Space

For more information and specific guides according to feature, see **Feature-Specific Requirements—Advanced*

Deployments *Section in System Requirements – Secret Server KB.*

Other Considerations

Virtualized Environments

Secret Server operates in a virtualized environment if it is configured on the Windows operating system. Hypervisors that the Secret Server can run on include: VMware, Hyper-V, VirtualBox, Xen, AWS, and Azure cloud environments.

Server Type

Do NOT install Secret Server on a domain controller. This restriction is a Microsoft limitation. ASP.NET does not operate reliably when installed on a domain controller.

Do NOT install Secret Server on a server that is running SharePoint.

Application Security

For maximum security, the application must be installed on a dedicated system. Secret Server can run on the same computer as other applications. Secret Server will still require sufficient RAM and CPU to operate normally. However, these applications must at least be applications of the same level of security and sensitivity so that access to these systems can be restricted. While all sensitive data in Secret Server is either securely hashed or encrypted, it is a security best practice to limit any opportunities for foul play.

More Disk Space

If you intend to use Session Recording, you must have more disk space for the database to store the recorded videos. Your storage requirements are based on frequency of usage, the applications recorded, and codec configured with Secret Server. For more information, see System Requirements – Session Recording .