Windocks Architecture and Security Review
Secure SQL Server Sandboxing

Windocks is an independent port of Docker's open source project to Windows, with container support for all editions of SQL server 2008 onward and database cloning. While Windocks preceded Microsoft's release of Docker support on Windows (Windocks was released in April, 2016), it's understandable that NIST and other industry reviews fail to comprehend the Windocks design. This article reviews the Windocks architecture and security provisions, with a focus on Windocks as a SQL Server container and database cloning solution (Windocks supports a "SQL Server Image only" configuration).

This document is organized in two sections: Section I introduces the Windocks architecture and security provisions with comparisons to other Docker implementations. Section II addresses issues and recommendations raised in NIST SP 800-190.

Summary:

Windocks is a port of Docker's open source project to Windows, supporting SQL Server containers and instances with database cloning. Windocks unique design preserves compatibility with existing enterprise systems and security processes, effectively addressing security concerns associated with Docker containers.

Windocks SQL Server containers are sourced from an "image" comprised of one or more locally installed SQL Server instance(s) that are cloned to create containers. Each SQL Server container is a conventional SQL Server named instance, with a non-virtualized file directory and registry settings. Windocks SQL Server containers are thus equivalent to conventional installed instances, and preserve compatibility with Active Directory Windows authentication, host and network firewalls, storage systems, and existing applications. Windocks avoids security concerns relating to public image repos, image complexity, namespace isolation, network complexity, and changes in enterprise infrastructure and processes.

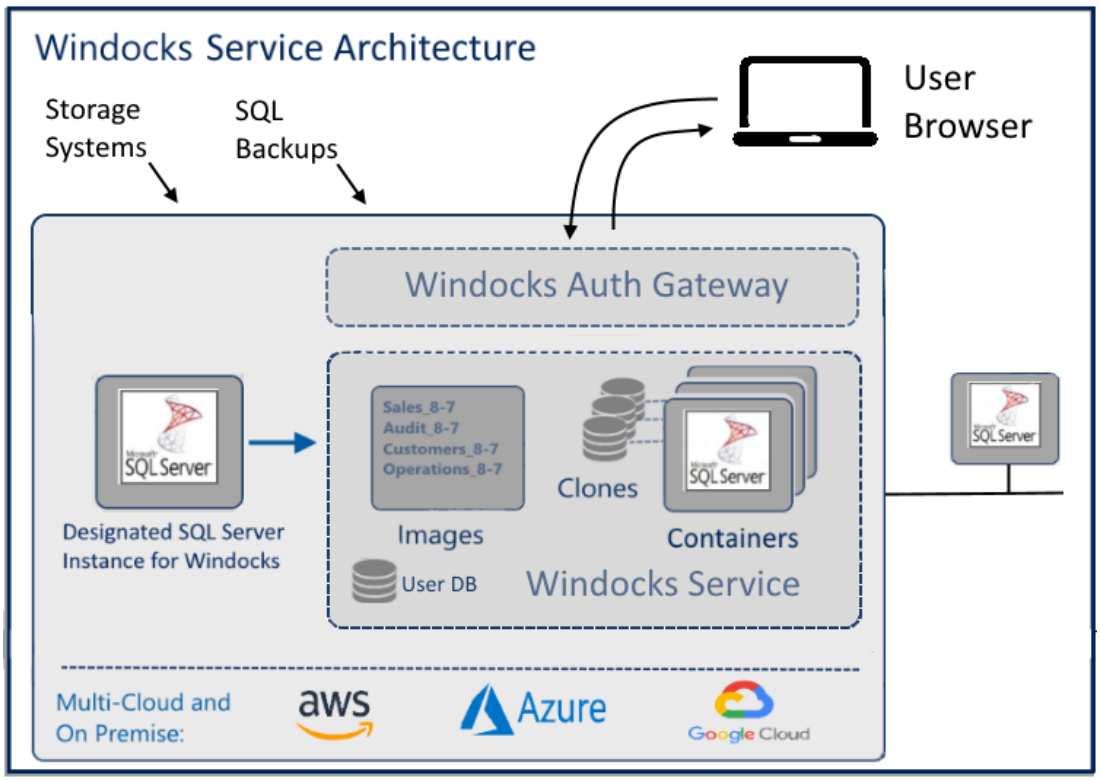
Windocks is a proven, hardened system that benefits from focused support of SQL Server containers and database cloning. Windocks SQL Server containers deliver secure enterprise support, using the well understood SQL Server object namespace isolation. Windocks includes an encrypted secrets store, support for SQL Server encryption and third party External Key Managers (EKM), and other provisions required for secure enterprise use. By focusing support on SQL Server containers, Windocks

avoids concerns over potential use of SSH, and sensitive docker commands (>docker exec) which are not supported by Windocks in a SQL Server only configuration.

Windocks automates use of enterprise infrastructure for database cloning with an application driven solution. SQL Server DBAs and developers are equipped to create, manage, and deliver containers and database clones, without involvement of storage array admins. Windocks images also enhances secure use of enterprise data by providing an authoritative data catalog with rich metadata for data governance, auditability, and reporting.

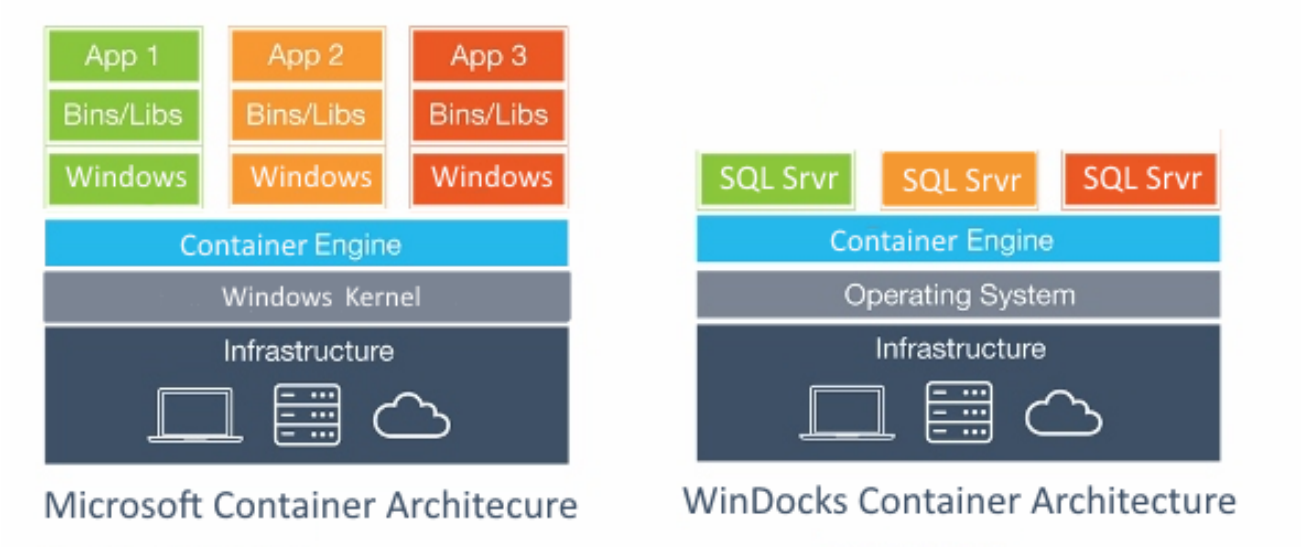
Section I: Windocks Architecture

The Windocks architecture is presented in the following three sections: Containers, Images, Database Cloning, and Services.



SQL Server Containers:

Windocks is an independent port of Docker's open source project to Windows, that runs on Windows Server 2012 R2 or Windows Server 2016, with image support for all editions of SQL Server 2008 onward, and .NET. Windocks is configurable to support SQL Server images only (the focus of this document), or can support SQL Server plus .NET and other open source images. SQL Server containers are each a SQL Server named instance with a local file directory and registry settings, running on a shared Windows operating system. This design preserves support for existing security processes and tooling within the enterprise.



Windocks focused support for SQL Server, with images based on locally installed instances that are cloned, and containers that include only the cloned SQL Server application yields many advantages:

Windows and SQL Server support: Windocks containers support Windows Server 2012 R2 and Windows server 2016, with all editions of SQL Server 2008 onward. This backward compatibility simplifies the use of SQL Server containers with existing systems and applications.

Compatibility with enterprise security processes and infrastructure: Windocks containers deliver the benefits of Docker software with high app density, speed, and interoperability with the Docker ecosystem, while preserving existing security and interoperability with existing and future Windows infrastructure. Windocks containers support Active Directory Windows authentication, Windows and Network based firewalls, and interoperate with existing applications and tools. Windocks does not call for wholesale changes in infrastructure as is common for other Docker implementations.

Maintainability: maintenance of most docker containers and images is complicated by operating system updates, which require containers and images to be rebuilt. Windocks containers and images are unaffected by Windows updates.

Scalability: Windocks containers are light-weight due to the lack of Windows operating system footprint, and offer roughly double the scalability compared to other Windows Docker containers. This scalability includes an effective “elastic databse pool” support, similar in performance to Microsoft Azure SQL Azure.

Licensing flexibility: Microsoft SQL Server containers are licensed as a Virtual Machines, with each non-developer SQL Server container requiring a minimum 4 CPU core license. Windocks containers are delivered as named instances on the host, and are allowed without additional licenses under existing Microsoft SQL Server licenses. This freedom is appealing for organizations using SQL containers with SSRS for production reporting.

SQL Server Images through Instance Cloning

Windocks images are based on locally installed SQL Server instances, and the long-standing provision in Microsoft licenses that allow for additional instances to be created by duplication (cloning). License compliance is an important topic, and we encourage readers to refer to Microsoft SQL Server licenses to understand these provisions.

Windocks is installed on a host that includes installed SQL Server instances, which are configured to support use as Windocks SQL Server images. Containers inherit parent instance attributes including edition capabilities, licensing, user logins, encryption keys and certificates, etc. Container creation takes approximately 15 seconds, and produces a new named instance with complete file directory and registry settings, that is managed with Docker commands and interoperates with existing applications and client tools. Once created, the container has no further dependence on the source instance/image.

The benefit of SQL Server instances as an image yields a number of benefits:

Image portability is achieved as any SQL Server release and edition can be installed on any of supported Windows operating systems, and interoperates on any public cloud or any Windows Server 2012 R2 or Server 2016. This portability contrasts with the lack of portability offered by Microsoft's Windows SQL Server images, which vary between Windows 10 and Windows Server 2016 base, and other Windows Server 2016 editions.

Ease of adoption and compatibility is facilitated with Windocks installation support for the past 10 years of SQL Server releases, and guaranteed interoperability with existing storage arrays and other Windows infrastructure.

Security is enhanced with a design that preserves interoperability with existing security tools and processes, including Active Directory Windows authentication, local and network based firewalls, and other tooling. Windocks design also avoids the many security concerns associated with other Docker implementations, which involve public image repositories, complex layered images, mis-configured images, and the requirement of new image scanning software and processes.

Database Cloning

Windocks includes unique SQL Server database cloning support for both Windows VHDs, and creation and management of clones from storage array snapshots. Windocks database cloning service supports clone delivery to any SQL Server environment, including Microsoft's SQL containers (both Linux and Windows), conventional SQL Server instances, and Windocks SQL Server containers.

Windocks database clones are built and managed as immutable SQL Server images, and include applied security policies, providing the enterprise with a single authoritative image for data access. The ability to provide an authoritative data catalog for organizational use dramatically improves the data sprawl that is common in most organizations. Windocks enhances database clone images with user/group authenticated access, and metadata on image creation date, security policies applied, and use history, providing the organization with insight into team cooperation, release frequency, and data auditability.

Windocks database cloning and images are a declarative system that automates use of storage infrastructure, enabling database administrators and qualified users to design, implement, and manage clones without involvement of storage admins. Windocks also manages the complete life cycle of all clones, and tracks the state of the end environment, storage volumes, VHDs, mount points, and state. On removal of the environment (or container), Windocks cleans up the complete environment. Windocks database clones consume very little storage, so the use of clones on existing storage arrays poses no "use tax" on this infrastructure.

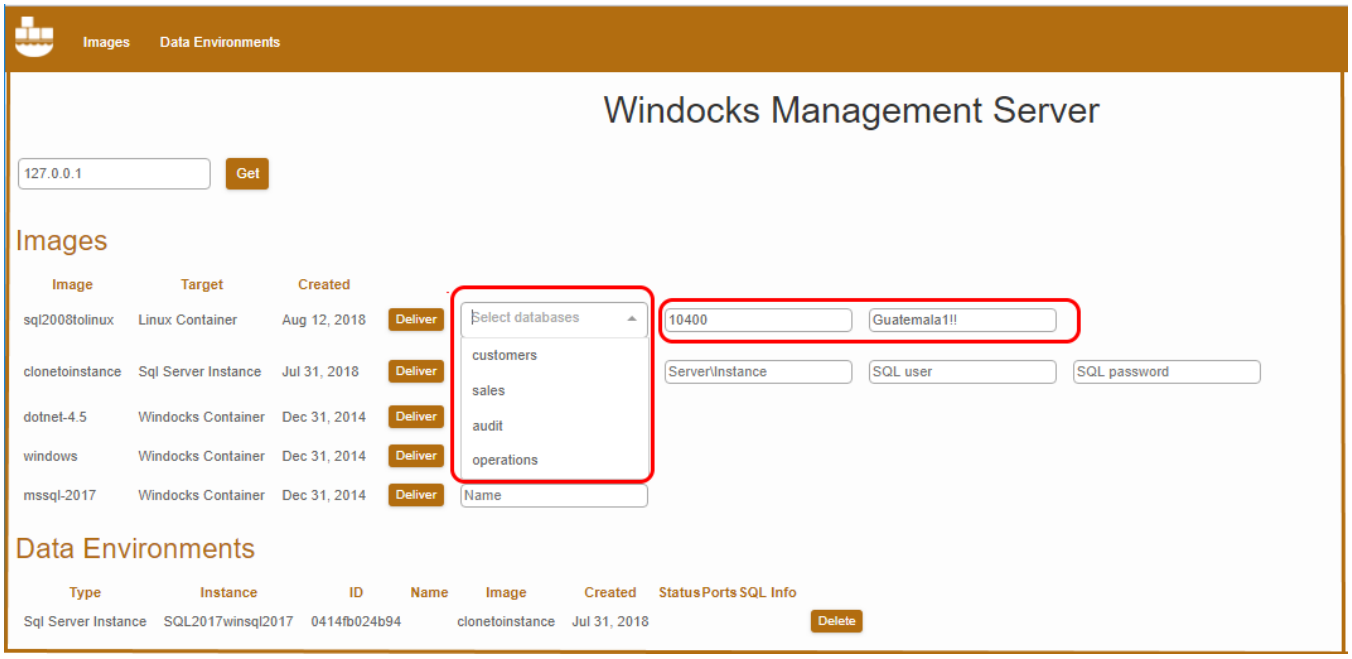
Windocks and User Authentication Services

The Windocks service combines support for containers and images with database cloning, and runs as a Windows Service. The User Authentication Gateway is a separate Windows service and Web UI that provides administrator and user support. The Windocks service is a complete port of Docker's open source project, and supports a subset of Docker commands consistent with the Windocks Service configuration (SQL Server only, or SQL Server plus .NET).

Windocks manages the complete lifecycle for each container and database clone, including the source VHD or snapshot, associated credentials, mount points, and state. On removal of the container or data environment, the associated VHD or volume array snapshot and associated mount points are cleaned up. A complete record of the clones, and user sessions is recorded, and forms the basis for enterprise data governance and auditability reporting.

Remote user support is provided through the User Authentication Gateway and web UI (image below), and replaces use of docker client software access via port 2375/76. The web UI provides user authentication and support to provision containers with clone database environments, and to start/stop, and remove containers, and is configurable to include SSL/TLS encryption. Access to containers is accomplished with normal client tools such as SSMS or other client applications. Administrators and approved developers can build images.

Automated operations are provided through PowerShell remote, which is Microsoft's preferred method for secure remote PowerShell operations. Alternatively, Docker API calls can be made using cURL, but are limited to the commands associated with building and managing SQL Server containers and images.



The Windocks and Windocks Auth services provide a number of security related advantages:

Docker based SQL Server sandbox, is a purposefully focused service that leverages the benefits of docker containers, while avoiding security concerns of complex images, docker client software accessing the host with docker exec and other commands.

Modern secure web UI supports http/https sessions, with user/role based access.

PowerShell remote, as Microsoft's preferred method for secure remote automation of systems, along with use of the exposed docker API subset via secure cURL sessions.

Data Governance and reporting is available with Windocks database of image creation and use, and will be enhanced to provide teams and management with insights to team cooperation, release frequency, and data image use.

Section II: Analyzing Windocks Support for NIST SP 800-190

The NIST Application Container Security Guide was published in September 2017, and outlines a series of concerns and recommendations for use of containers. See https://doi.org/10.6028/NIST.SP.800-190

This section reviews the concerns outlined in the NIST paper. The Windocks response to each concern is listed as Fulfilled, Partially Fulfilled, or as Not-Applicable (N/A).

Public image repositories are a concern due to unvetted public contributions, misconfiguration, and a potential source of malware.	**N/A:** Windocks images are based on locally installed SQL Server instances, which comply with enterprise configuration review and audit.
Layered Docker images are a concern due to complexity, combining Operating System, libraries, and application code. Complexity and the need for security has led to new image scanning tools.	**N/A:** Windocks images are simply clones of IT vetted and licensed software, and do not represent a new form of software distribution or need new "scanning." Database clones are likewise simply existing SQL Server databases, with security policies applied in the form of SQL Scripts and other preparations, accessed via Windows file system (VHDs), or from existing storage volumes. These images can easily be audited using existing tools.
Recommended image scanning	**N/A:** as outlined in the previous points, Windocks makes use of existing vetted SQL Server instances, and avoids the complexity and security risks of public repos and layered images.
Recommended separation of containers on different hosts	**Fulfilled:** Windocks is easily deployed and managed on different hosts to separate developers, testers, and other functional teams.
Recommended use of run-time defense for intrusion detection.	**Fulfilled:** Windocks supports intrusion detection and other security tools within the enterprise today.

Namespace and Container isolation is a concern that originated with early docker releases that container users to gain administrative privileges.	**Fulfilled:** Windocks isolation is based on the secure SQL Server object namespace. There are no risks of users escalating privileges to attack the system or other containers, as the SQL Server container is limited to databases and SQL scripts. Windocks also supports configurable SQL Server containers with no sa passwords, or encrypted sa passwords.
Credential secret management is a concern due to dockerfiles often including sensitive credentials.	**Fulfilled:** Windocks includes built-in encrypted secrets support, so that account credentials are protected.
User Authentication is a concern as standard docker clients are not authenticated (Docker Enterprise Edition includes authenticated session support)	**Fulfilled:** Windocks includes user authentication support.
Container resource governance is a concern as poorly designed containers can escalate their resource demands to disrupt system operation	**Fulfilled:** Windocks addresses this by both focusing support on SQL Server containers with both container resource governance and native SQL Server instance resource governance.
Encrypted user network traffic	**Fulfilled:** Windocks supports SSL/TLS certificates for authenticated user sessions.
Encrypted container network traffic via overlay networks	**Fulfilled:** Windocks does not employ the complexity of overlay networks, or enforce the use of encryption other than chosen by the enterprise with normal SQL Server encrypted network support.
Image Immutability	**Fulfilled:** Windocks images are immutable reflecting standard Docker behavior.
Mis-use of Docker commands	**Fulfilled:** Windocks focused support for SQL Server containers and database cloning avoids concerns over use of SSH, and commands such as >docker exec.
Data Persistence and Image meta-data	**Fulfilled:** Windocks supports use of Windows VHDs and storage arrays to provide persistent data to containers and conventional SQL Server instances. Windocks provides superior data governance and security, with meta-data attached to images, for audits and reporting.
Minimal OS footprint is recommended by NIST to minimize attack surface	**Fulfilled:** Windocks use of the Windows Server operating system is optimal, as this design achieves dramatic reductions in attack surface with up to 30+ containers on a single host compared to 30 + VMs. Other benefits of supporting the standard Windows Operating System are highlighted throughout this document.

Image proliferation is a concern where images can become ultimately numerous, and due to the layered designs, require ongoing image scanning.	**N/A:** Image proliferation is a non-issue as each image is based on the known SQL Server configuration. The only differences between images are from the source databases, and SQL Server scripts applied.
Data persistence and governance is a concern over control of data images or volumes being used by container users.	**Fulfilled:** Windocks puts DBAs and select developers in control of building database clone images, and supports use of the images with all SQL Server environments, providing an authoritative catalog of images that can be audited and reported.

Learn more

Explore how Windocks supports SQL Server 2017 Linux containers, and other topics.

Explore database clone delivery to SQL Server 2017 Linux containers, and Windows SQL Server instances:

https://windocks.com/files/docker-sql-server-containers%20-linux-clone-for-sql%20server-2017.pdf

https://windocks.com/files/sql-server-database-cloning%20for-sql-server-instances.pdf

Explore support for External Key Managers and TDE:

https://windocks.com/files/sql-server-containers-and-extensible-key-managers-EKM.pdf

https://windocks.com/files/WindocksSQLServerContainersAndTDEEncryptedDatabases.pdf

Configure secure file sharing with NFS and how Windocks supports Pure Storage arrays:

https://windocks.com/files/NetworkFileSharesForWindocks.pdf

https://windocks.com/files/pure-storage-cloning-san-docker-containers.pdf

Advanced T-SQL scripting options and integration with Git:

https://windocks.com/files/sql-server-scripts-for%20-images-and-containers.pdf

https://windocks.com/lps/gitbuildtest

Support

We appreciate feedback and feature requests. Email support@windocks.com with your suggestions and for for technical support.

About Windocks

Windocks combines Docker Windows containers with SQL Server database cloning, for a modern, open data delivery solution. Enterprises modernize application development, testing, reporting and BI with existing licenses and infrastructure, at a fraction the cost of alternatives.

For additional information, visit www.windocks.com, or contact Windocks at info@windocks.com

Windocks
Data Delivered

amazon web services | Partner Network

Microsoft Partner

docker
MEMBER

PURESTORAGE PARTNER