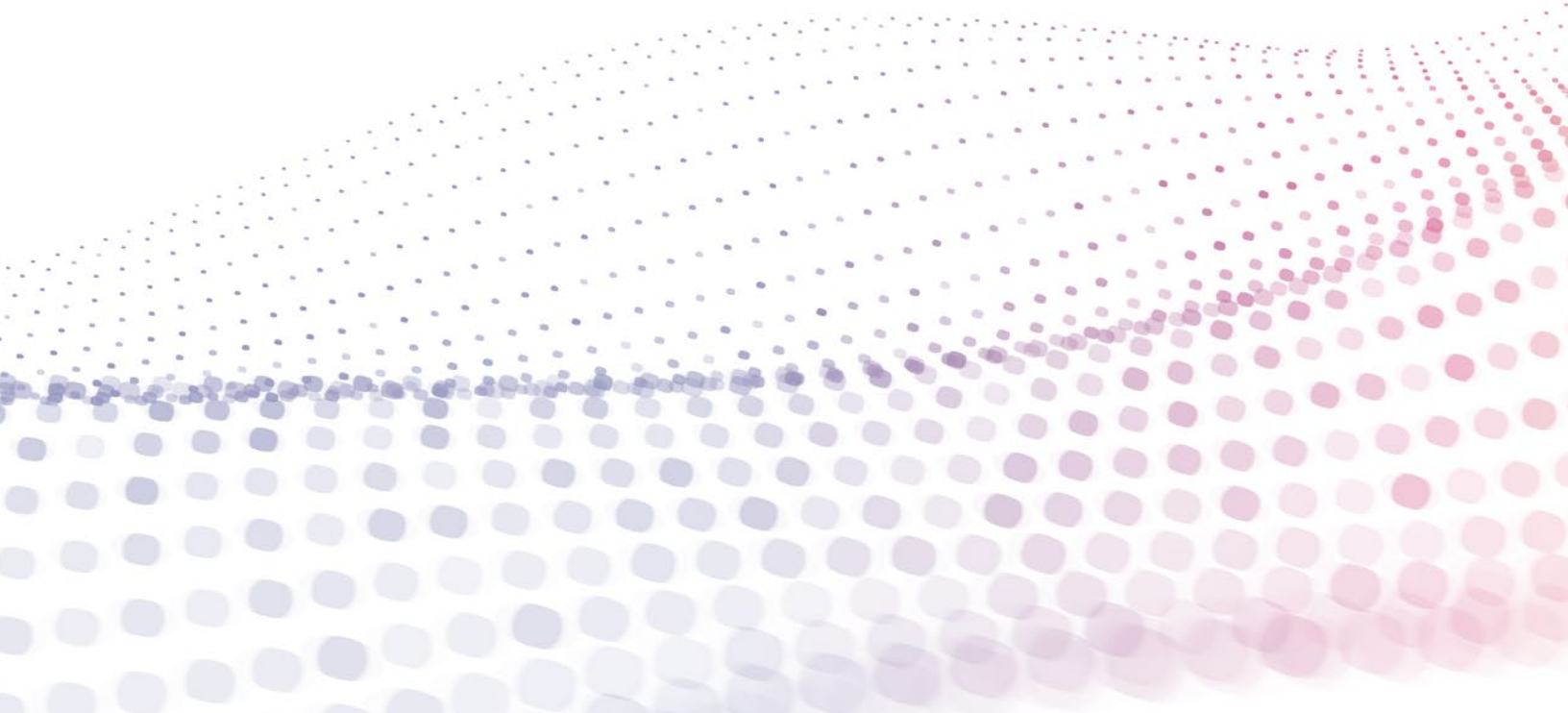
MarkLogic®

Secure Architectures When Deploying MarkLogic On-Premises

MARKLOGIC WHITE PAPER · JULY 2018

Maintaining security in your MarkLogic deployment architecture is critical—whether you are deploying a 3- or 30-node cluster. Relying on best practices gleaned from hundreds of actual implementations, this white paper provides recommended architectures and checklists to reference when deploying MarkLogic securely into on-premises infrastructure.



Contents

Introduction 1

Security Considerations for On-Premises Deployments 2

Authentication
Authorization & Access Control
Auditing
Communications Security (Data in Flight)
Security of Data on Media (Data at Rest)
Backup Data Security
Application Configuration Security
Environment Security

Classifying Your Deployment 5

Deployment Size Classification 5

Small Deployments
Medium Deployments
Large Deployments
Extra Large Deployments

Security Profile Classification 7

Standard Security Profile
Medium Security Profile
High Security Profile

Deployment Checklists 8

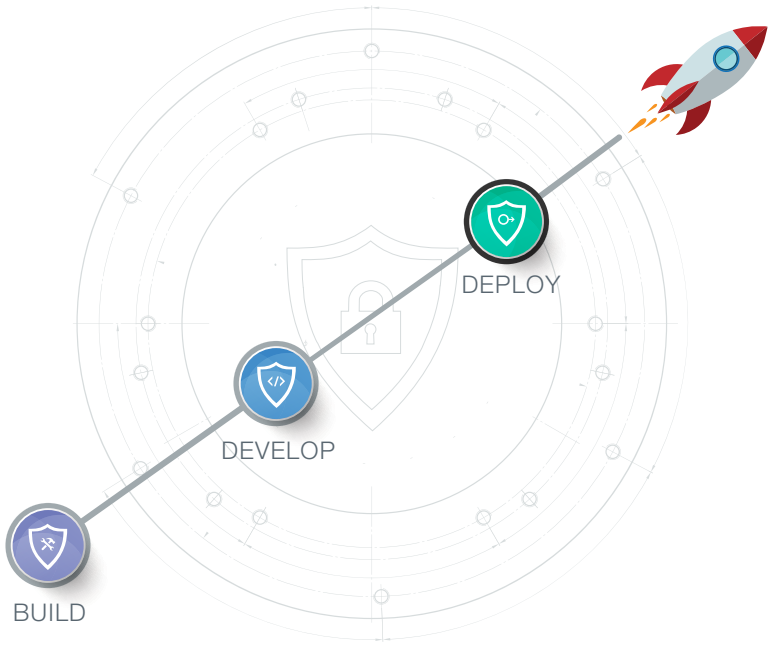
Small Deployment Environments
Medium Deployment Environments
Large Deployment Environments
Extra Large Environments

Available Assistance 18

Documentation
Training
Support
Consulting Services

Conclusion 19

Key Resources



Introduction

Maintaining security through the deployment process is critical—all the way from planning to going live into production. Our overall approach to security involves looking at an integrated security ecosystem so that organizations can deploy MarkLogic securely while maintaining complete peace of mind.

The MarkLogic security ecosystem is framed by three main components: (1) How We Build a Secure Product, (2) How to Develop Secure Applications on MarkLogic, and (3) How to Deploy MarkLogic Securely. There are other security white papers that provide an overview of each of those three components. This guide goes even deeper on that third aspect: How to deploy MarkLogic securely.

In this white paper, we take a close look at on-premises deployments of different sizes—small, medium, large, and extra large. Then, we look at the security profiles—standard, medium, and high. For example, you may have a "medium sized deployment with a high security profile." Depending on which type of deployment you have, we provide the recommended architectural design and checklist for that scenario. In the section on classifying your deployment, we walk through the characteristics of the various profiles.

Our recommendations take into careful consideration the most important aspects of security—authentication, authorization, auditing, and more. We also take into account how a MarkLogic deployment might fit into your existing security infrastructure. For example, some organizations already have an identity or key management system in place.

All of the information provided in this white paper is based on best practices developed from our experience with hundreds of MarkLogic deployments at large enterprises, and we expect this information will help architects, DBAs, and System and Infrastructure Administrators ("SysOps") make the right decisions during the deployment process.

Security Considerations for On-Premises Deployments

While security threats and the necessary precautions to protect your data against those threats will always evolve, there are a generally agreed upon set of considerations that every organizations needs to pay close attention to when deploying MarkLogic on-premises. Those considerations are listed here, and we refer to them throughout the rest of this white paper.

Authentication

Most enterprises have an Identity and Access Management (IdAM) system, whether it is Active Directory, LDAP, or some other system. The goal of a centralized IdAM system is to manage the users in the enterprise in a consistent and secure way. So, when a user is authenticated in the enterprise it is clear who the authenticated user is regardless of the application or tools they plan to use.

MarkLogic provides support for authenticating users against IdAM systems using external authentication protocols such as LDAP, Kerberos, and PKI-based systems. MarkLogic does have basic built-in functionality to do local user management, but we recommend using external authentication with an enterprise IdAM system. We also recommend implementing strong authentication using certificates instead of using simple password-based authentication.

Authorization & Access Control

Centralized IdAM systems are also frequently used in large enterprises for managing common access control policies that apply to all users. These policies can then be uniformly enforced across all applications. In addition to common access control policies, an individual application group might define access control policies that grant access to specific functionality in that application group depending on the set of applications that a subset of users need access to. The effective policy that is enforced for a particular authenticated user is the sum of the common policy and the application specific policy that is defined for that user.

MarkLogic has very granular, flexible access control policy support with Role Based Access Control (RBAC), Attribute Based Access Control (ABAC), and Policy Based Access Control (PBAC). MarkLogic also supports enhanced security mechanisms like Compartment Security and Element Level Security. When configured with external authentication, common access control policies like group and organization membership can be enforced by MarkLogic in addition to access control policies that are defined directly in MarkLogic.

Auditing

Most large enterprises, for compliance reasons, have a requirement to ensure that the right user is authenticated with the right policy, and is granted access to the right set of resources that the user is entitled to. This ensures that users are given *only* the right amount of access, no more and no less.

MarkLogic has an extensive set of auditable events, which enables organizations to satisfy their auditing requirements. The MarkLogic Administration Guide lists all the auditable events that can be configured in MarkLogic. The list of auditable events includes things like authentication failures, queries that were run, permissions changes, and much more. It is also possible to restrict audit events based on various identities (user, role, or document URI).

Communications Security (Data in Flight)

In addition to requiring strong authentication and granular authorization policies, most large enterprises require secure communication channels for data in flight (sometime called transport security or data in motion) between various services and the various client applications or endpoints. This is typically done with SSL/TLS and needs to be mutually authenticated.

Most enterprises rely on third party Certificate Authorities (CAs) to issue and manage the certificates required for transport security. But, they may also deploy their own internal CAs to provision and issue the certificates that are used to secure the communication channels. These internal CAs can be intermediate CAs or root CAs. An intermediate CA, also called a Registration Authority (RA), is authorized by a third party CA to issue certificates on its behalf within the enterprise. A root CA is a CA that provides the trust anchor utilized by intermediate CAs in the same chain. A root CA can be self-signed by the enterprise or can use a third party CA as the source of trust. MarkLogic supports both models.

We strongly recommend that organizations use mutual authentication to secure communication channels between various services and clients, including MarkLogic and its clients. MarkLogic can support both kinds of certificate authorities—root/self-signed CAs and third party CAs. MarkLogic ships with a standard list of commonly recognized third party root certificates that can be used to validate certificates issued by the corresponding third party CA. In the event that the organization is a root CA to a third party CA, the intermediate root certificate should be added to MarkLogic so it can validate both the third party root CA and the enterprise root CA via a chain in order to secure communication channels. In the event the organization itself is the root CA, then this root CA has to be imported into MarkLogic in order to validate certificates issued by the enterprise root CA.

In addition to supporting third party CAs and root CAs, MarkLogic can be configured to be the root CA for itself and its clients. However, we do not recommend this approach and it should be viewed as the last option when other more preferred options are not available.

Security of Data on Media (Data at Rest)

Enterprises require their users and applications to be secure. To secure applications, they may need to secure the application data where it is stored on disk or on removable media. If this is a requirement, the organizations may use a variety of mechanisms, such as Full Disk Encryption (FDE), Transparent Data Encryption (TDE), or application/native encryption. MarkLogic supports all of these mechanisms: FDE, TDE, and application/native encryption.

In the case of FDE and TDE, since the encryption is external to MarkLogic, no configuration is required. In fact, MarkLogic itself is not aware of the mechanism. If an organization chooses to use application/native encryption, then MarkLogic can be configured to support this by using an external Key Management System (KMS) or MarkLogic's own internal Key Management System (KMS). For most large organizations, we recommended using an external KMS with MarkLogic. For example, MarkLogic supports the use of the AWS Key Management Service (KMS). If using an external KMS is not possible, then the organization can rely on MarkLogic's internal KMS system, FDE, or TDE.

Backup Data Security

Enterprises need to encrypt data used in production systems, that is a given. But, some organizations do not adequately secure the backups. There is often data from production systems on backup storage media or removable media that is left unsecured.

To secure backup data with MarkLogic, organizations can use an external Key Management System (KMS), MarkLogic's own internal KMS, Full Disk Encryption (FDE), or Transparent Data Encryption (TDE). If using an external KMS to secure production data, the same system can be used to secure MarkLogic backup data. If the MarkLogic internal KMS is used, then MarkLogic generates the keys that are required to backup and restore the encrypted data. In this case, MarkLogic supports backing up the encrypted data and the backup keys separately, as well as backing up the encrypted data and the keys as a single payload.

Application Configuration Security

Even if an organization properly secures the users, applications, and data, it is easy to forget about the set of capabilities enabled by application configuration. Applications have their own logs and operational data-in-use. It is important to also secure that data.

MarkLogic is designed to secure not only the application data, but also secure its logs and configuration data. To do this, MarkLogic uses the same mechanisms that are used to secure application data. We strongly recommend that organizations configure MarkLogic to secure the application databases and MarkLogic internal system databases such as the MarkLogic Security database.

Environment Security

Lastly, organizations must secure the environment in which their applications and data are used. Environment security can be classified into two categories: System/host security and application security. System/host security is about securing the operating systems (OS), ports, and services. Application security pertains to running application code itself, communication between applications, and the ports and tools used by applications.

For system/host security, it is a good hygiene to:

1. Keep the operating system and all system tools up to date with the latest patches and component versions in order to address any potential security issues.
2. Uninstall or remove tools packages or applications that are not required on the host or system for normal operations.
3. Disable all unused ports or background services that are not required for normal operations on the system or host.
4. Ensure services that have the option to run on secure ports should be so configured by default and should be used (e.g., HTTPS).
5. Ensure machine-to-machine communication channels are mutually authenticated and secure.

For application security, it is good hygiene to:

1. Keep all applications up to date with the latest security patches and application patches.
2. Ensure all communications between application either using standard protocols or application specific proprietary protocols. And, ensure that communications are mutually authenticated.
3. Disable all unused application ports and secure all ports that are used by the applications.
4. Delete tools installed by applications that are not used in normal operations, especially those that are utility applications that are installed on the systems/host.
5. Ensure that applications are using the latest versions of third party and open source components to minimize the possibility of potential open source security issues.

The MarkLogic Administration Guide lists these and other recommendations on how to secure the environment into which you plan to install MarkLogic.

Classifying Your Deployment

Now that we have covered the general list of considerations to look at, it is time to get more specific about *your* deployment. The below grid classifies different deployments based on size and security profile.

Depending on the size of your deployment, we provide guidance to ensure that your system is properly secured depending on the security profile. For example, a large deployment with considerable amounts of data for a mission-critical system requires a high security profile. Once you have characterized the size and security profile for your deployment, you can skip to the appropriate checklist.

		Security Profile		
		Standard	**Medium**	**High**
Deployment Size	**Small**	Required	Recommended	Optional
	Medium		Required	Recommended
	Large			Required
	Extra Large			Required

Deployment Size Classification

While deployment environments are classified into four sizes—small, medium, large, and extra large from an architectural and design perspective—it is easy to migrate from a smaller to larger size (going from small to medium), or a lower to higher profile (going from medium to high). In other words, our recommendations are designed to build on each other so that as your system grows, you can make it more and more secure. However, we do not recommend going in the opposite direction, regressing from a high security profile to a standard security profile. For that case, we recommend setting up a new environment with the right security profile independent from the existing environment.

Small Deployments

The general characteristics of a small deployment, by MarkLogic standards, are the following:

- Data size from 1 – 3 TB
- 3 node cluster with or without external authentication
- Could have multiple clusters each with 3 nodes
- Advanced Encryption is optional
- External KMS is optional

Medium Deployments

The general characteristics of a medium deployment, by MarkLogic standards, are the following:

- Data sizes from 3 – 100 TB
- Multi-cluster environment with 3 to 10 clusters
- Ops Director for cluster management is optional
- Advanced Encryption is in use
- External KMS is optional
- Integration with SAML based Single Sign-On (SSO) is used to achieve tight integration with enterprise SSO with partitioned application level policy management

Large Deployments

The general characteristics of a large deployment, by MarkLogic standards, are the following:

- Data size is 100 TB or more
- Large cluster environment with multiple regions or locations
- Enterprise HA/DR is in use
- Ops Director for cluster management is used
- External KMS is used
- MarkLogic is part of the larger security architecture that has centralized policy management and centralized compliance policies enforced by applications

Extra Large Deployments

The general characteristics of an extra large deployment, by MarkLogic standards, are the following:

- Data size is usually one or more petabytes
- The environment spans multiple geographic regions worldwide, with a global security data center to centrally manage security policies
- The considerations of the security profile are customized to each geography and the data security requirements (regulatory and compliance) for that local jurisdiction are taken into account
- The environment has localized infrastructure management and non-local administrators only have access to monitor each localized geography

Security Profile Classification

Standard Security Profile

With a standard security profile, there is not much additional effort required to enhance data security. A standard security profile is appropriate in environments where the data and application that is serving the data is already public. Another case may be that there is already a dependable air gap isolation that lowers the risk. Another case may be that it is a testing environment (for the purposes of integration projects or scalability tests for example) where precautions have already been taken to anonymize the data. In these cases, there is a low risk associated with potential data leakage and so a standard security profile is appropriate.

- Authentication controls should still be in place in spite of the standard security profile. The default authentication mechanism could be local user or an isolated IdAM system for air gapped environments.
- Authorization controls (may not be very granular or extensive) should be in place to monitor access in the event it becomes necessary. We also recommend using "least privilege" access by default with broad access being granted as a defined security policy.
- Even though there may be no global policy enforcing auditing requirements, applications should have the default settings in place.

Medium Security Profile

A medium security profile has the following characteristics:

Authentication – Preferred authentication method is a department or enterprise wide user managed repository. The level of authentication can be passwords or some form of SSO based technology like Kerberos, LDAP, or SAML.

Authorization – The authorization policy management is entirely up to the application. There are very minimal to no global security policies that need to be enforced uniformly across all applications. While it is still application level authorization, it is imperative that "least privilege" access is still the default with application administrators providing the enforcement policy definition.

Auditing – There is no global policy enforcing auditing requirements but applications should have the default setting with some additional auditing controls in place defined by the application administrator.

Environment/Communications Security – In this security profile, the environment is managed by an application administrator who has full administrative access to the single application being managed. Communication/network security is also managed locally with either self-signed certificates or a local Registration Authority that can be managed by the application administrator. Since the environment is managed by a single application administrator, there is little to no need for a single management console such as MarkLogic Ops Director unless the data management environment is on the higher end of the scale. Even in this case, the application administrator has complete and full access to the application and environment management domain.

Data Security – The data value is higher than in the standard security profile but it is not high enough that there is a need to define and enforce a global data security policy. The applications decide on the nature of the data and controls necessary. Encryption of data could be localized using a self-contained KMS system managed by the application administrator.

High Security Profile

A high security profile has the following characteristics:

Authentication – The preferred authentication method is an enterprise-wide user managed repository. The level of authentication is usually a strong credential-based system like certificates or smart cards. But, authentication can also be passwords or some form of SSO based technology like Kerberos, LDAP, or SAML with stringent credential management policies.

Authorization – The authorization policy management is a hybrid model where there are global security policies defined by the enterprise security administrator that must be enforced uniformly across the enterprise application ecosystem. It is still possible that application level authorization is defined by the application administrator but in that case it is imperative that the access by "least privilege" is still the default with the application administrator providing the enforcement policy definition. Global security policies prohibit the application administrator from defining application level policies that conflict or over-ride the global policy. Such enforcement is usually audited by the global security group on an application by application basis.

Auditing – There is a global policy enforcing audit requirements and all applications can choose to define audit controls in addition to the global policy. However, all applications should have the default setting with additional audit controls in place defined by the application administrator. There is usually a centralized audit mechanism in place that collates and monitors the compliance policies.

Environment/Communication Security – The environment is managed by the enterprise administrator who has full management access. The application administrator has little to no local access. Communication/network security is managed globally with either a third party CA or a local Registration Authority (RA) that can be managed by the enterprise administrator. In the case of the local RA, it is still rooted by an external third party CA. Since the environment is managed by an enterprise administrator, there is usually a single management console like MarkLogic's Ops Director that is monitored and managed by the enterprise administrator from a security perspective. Application level management is delegated to the application administrator and all access is audited by the enterprise administrator. The enterprise administrator still has complete and full access to the application and environment management domain while delegating access to the application administrator.

Data Security – The data value is higher than in the medium security profile so there is a need to define and enforce a global data security policy. The global security policy defines what applications will enforce data security based on the nature of the data and controls. Data encryption is mandatory and an external KMS system managed by the enterprise administrator is deployed centrally.

Deployment Checklists

Now that you have classified your deployment by size and security profile, you can skip to the appropriate deployment checklist. You will notice that the architectures and requirements build on each other, with a logical progression from less complexity for small deployments carrying a standard security profile to more complexity (and more security) for larger deployments.

The bullets in each checklist are **Required** steps unless noted as being **"Recommended"** or "**Optional**". Here is how we define each:

- **Required** – Basic, minimal security requirements
- **Recommended** – Industry standard security best practices
- **Optional** – Even higher security controls for more specialized situations

Small Deployment Environments

Standard Security Profile in a Small Environment

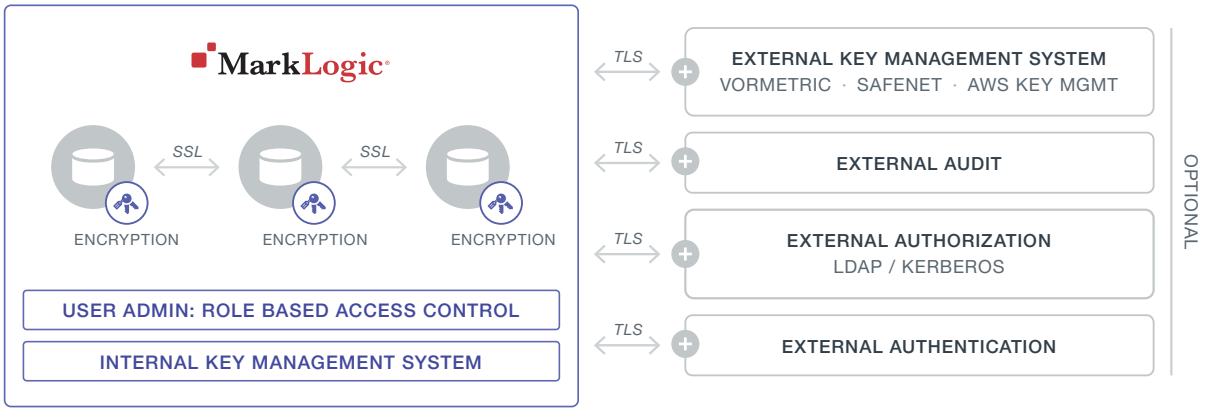


Figure 1: Architecture for a standard security profile in a small deployment.

Authentication – Host/System Security

1. If local authentication is chosen, then ensure that the Admin account on machine is well protected
2. Disable or delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy
4. Ensure that no user accounts are shared
5. Limit group membership on the hosts to valid users
6. If domain or external authentication is selected, ensure a minimum number of valid local accounts are allowed
7. Ensure system is hardened

Authentication – MarkLogic Application Users

1. Configure and harden MarkLogic application server
2. Recommended: Configure external authentication for all MarkLogic users
3. Optional: Configure communication security, preferably using third party issued SSL/TLS certificates

Authorization – External/Host

1. If using external authorization, ensure that group membership is limited and updated
2. If using OS level groups, ensure those are limited and updated
3. Recommended: Remove unused and generic groups for both host-based authorization and group authorization

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privilege feature to limit access to resources

Auditing – External/Host

1. Recommended: Ensure that auditing is enabled at the system level
2. Recommended: Ensure auditing is enabled for external authentication if using external authentication

Auditing – MarkLogic

1. Recommended: Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Optional: Enable encryption of data at the storage or disk level if available
2. Optional: Enable MarkLogic's internal vault to encrypt MarkLogic data files. Select log and config encryption

Backup Data Security

1. If data and the wallet are backed up separately, ensure they are backed up atomically
2. If doing a manual backup, ensure that backups are password protected and encryption is enabled
3. Recommended: Ensure backup policies are in place for MarkLogic data

Medium Security Profile in a Small Environment

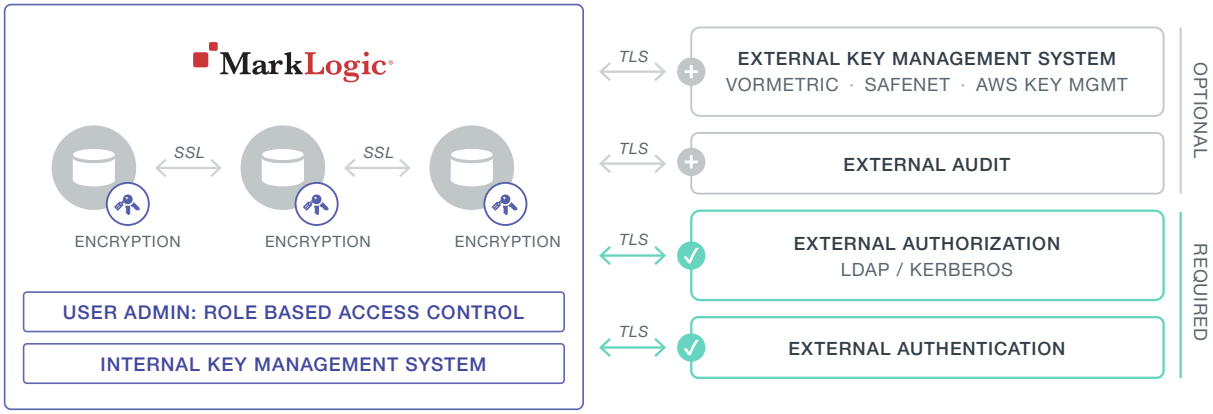


Figure 2: Architecture for a medium security profile in a small deployment.

Authentication – Host/System Security

1. Local authentication is not recommended. But, if it is used, then ensure the Admin account is well protected
2. Disable or delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy
4. Limit group membership on the hosts to valid users
5. Domain or external authentication is required. So, ensure a minimum number of valid local account are allowed. (Optional: Enable Single Sign-On (SSO) for users)
6. Ensure system is hardened

Authentication – MarkLogic Application Users

1. Configure external authentication for all MarkLogic users
2. Configure and harden MarkLogic application server
3. Recommended: Configure communication security with SSL/TLS using third party issued certificates.

Authorization – External/Host

1. If using external authorization, ensure that group membership is limited and updated
2. If using OS level groups, ensure those are limited and is updated
3. Remove unused and generic groups for both host based authorization and group authorization

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privilege feature to limit access to resources

Auditing – External/Host

1. Ensure that auditing is enabled at the system level
2. Ensure auditing is enabled for external authentication if external authentication is used

Auditing – MarkLogic

1. Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Enable encryption of data utilizing MarkLogic's internal KMS. (Optional: Select log and config encryption)
2. Recommended: Enable encryption of data at the storage or disk level
3. Optional: Use an external KMS to manage encryption keys (requires Advanced Security option)

Backup Data Security

1. Ensure backup policies are in place for MarkLogic data
2. If doing a manual backup, ensure that backups are password protected. Optional: Enable encryption
3. If data and wallet are backed up separately, ensure that they are done atomically

High Security Profile in a Small Environment

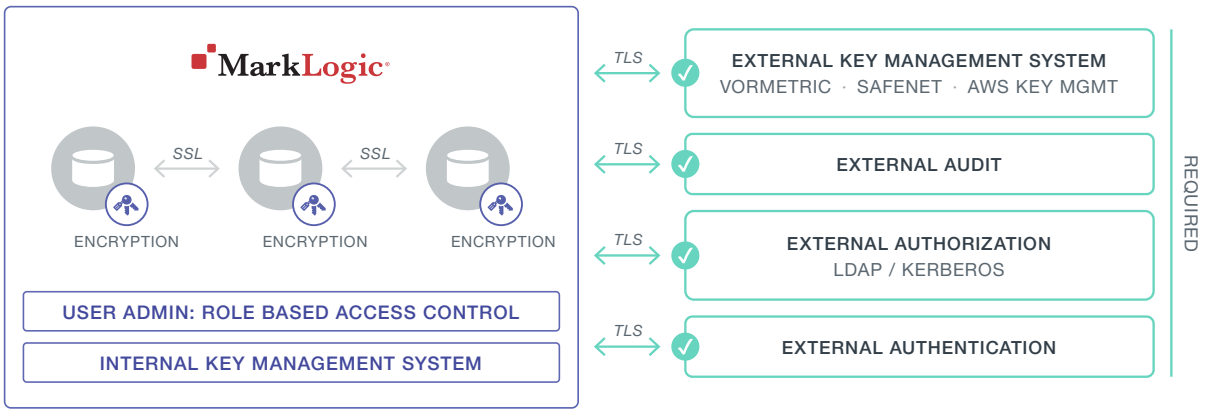


Figure 3: Architecture for a high security profile in a small deployment.

Authentication – Host/System Security

1. Centralized, external authentication must be used for user authentication; the admin account must be well protected
2. Disable or delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy
4. Limit group membership on the hosts to valid users
5. Domain or external authentication is required. SSO services may be deployed as well, centralized authorization policies may be deployed as well
6. Ensure privileges are granted by mapping roles to privileges and roles to users (RBAC) so that privileges can be globally managed
7. Ensure system is hardened

Authentication – MarkLogic Application Users

1. Configure external authentication for all MarkLogic users
2. Configure communication security using third party issued SSL/TLS certificates (Do not use self-signed certificates)
3. Configure and harden MarkLogic application server

Authorization – External/Host

1. Require external authorization, and ensure that group membership is limited and updated regularly
2. If using OS level groups, ensure they are limited and are updated regularly
3. Remove unused and generic groups for both host-based authorization and group authorization

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privileges and roles limit access to resources

Auditing – External/Host

1. Ensure that auditing is enabled at the system level
2. Ensure auditing is enabled for external authentication if external authentication is used

Auditing – MarkLogic

1. Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Enable encryption of data at the storage or disk level if available
2. Use an external KMS to manage encryption keys (requires Advanced Security option)

Backup Data Security

1. Ensure backup policies are in place for MarkLogic data
2. If doing a manual backup, ensure that backups are password protected and encryption is enabled using a Backup Encryption Certificate provisioned by the external KMS
3. If data and wallet are backed up separately, ensure that they are done atomically

Medium Deployment Environments

Standard Security Profile in a Medium Sized Environment

In a medium sized deployment that consists of multiple clusters with many databases, we recommend that it be configured with a medium or high security profile. The controls in a standard security profile environment are not strong enough, creating unnecessary risk. The only exception to this would be an environment used exclusively for development or testing. In that case, it must not contain production or live data (anonymized or simulated data sets are acceptable). If such a security profile is indeed deployed, all optional checklist items should be implemented during deployment.

Medium Security Profile in a Medium Sized Environment

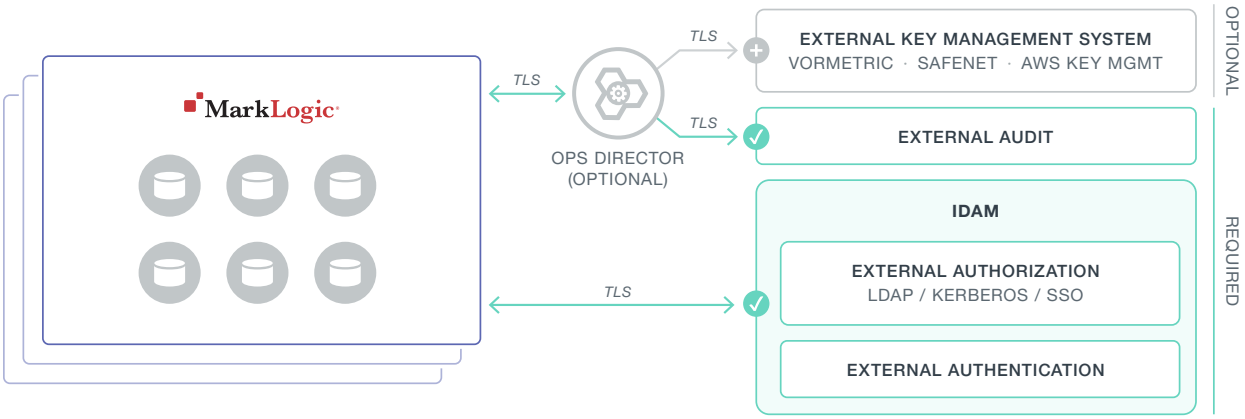


Figure 4: Architecture for a medium security profile in a medium deployment.

Authentication – Host/System Security

1. Ensure that the Admin account on the machine is well protected by means of strong authentication (Local authentication must not be used)
2. Disable or delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy
4. Enforce group membership on the hosts to valid users
5. Domain or external authentication is required to ensure minimum number of valid local account are allowed. (Optional: Enforce strong authentication for users)
6. Ensure system is hardened
7. Optional: Enforce strong authentication controls

Authentication – MarkLogic Application Users

1. Configure external authentication for all MarkLogic users optionally using strong authentication
2. Inter-cluster communications should be secured with mutual authentication
3. Configure and harden MarkLogic application server
4. Recommended: Configure communication security with SSL/TLS using third party issued certificates
5. Optional: Deploy and use Ops Director to manage the MarkLogic ecosystem. Ensure Ops Director is secured to a similar security profile as all other applications

Authorization – External/Host

1. If using external authorization, ensure that group membership is limited and updated
2. If using OS level groups, ensure they are limited and updated regularly
3. Remove unused and generic groups for both host based authorization and group authorization

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privileges and roles to limit access to resources

Auditing – External/Host

1. Ensure that auditing is enabled at the system level
2. Ensure auditing is enabled for external authentication if external authentication is used
3. Recommended: Integration with enterprise auditing tools

Auditing – MarkLogic

1. Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Recommended: Enable encryption of data at the storage or disk level
2. Recommended: Enable encryption of data utilizing MarkLogic's internal KMS. (Optional: Select log and config encryption)
3. Optional: Use an external KMS to manage encryption keys (requires Advanced Security option)

Backup Data Security

1. Ensure backup policies are in place for MarkLogic data
2. If doing a manual backup ensure that backups are password protected and optionally encryption is enabled
3. If data and wallet are backed up separately, ensure that they are done atomically
4. Optional: Enable encryption utilizing MarkLogic internal KMS or, even better, an external KMS

High Security Profile in a Medium Sized Environment

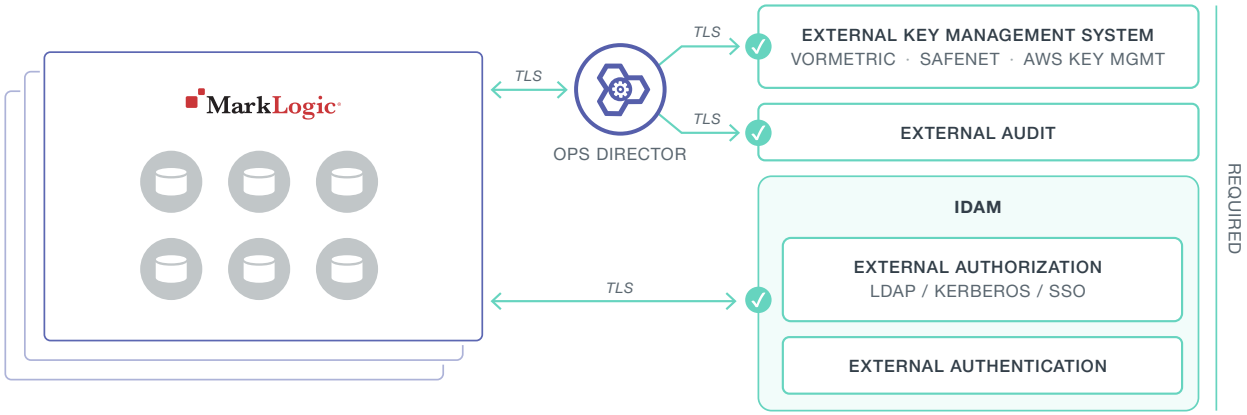


Figure 5: Architecture for a high security profile in a medium deployment.

Authentication – Host/System security

1. External/Network login to be chosen for user authentication. Ensure admin account on machine is well protected using strong credentials. Hosts may optionally be authenticated as resources within the enterprise
2. Disable or delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy along with strong authentication enforcement
4. Limit group membership on the hosts to valid authenticated users
5. Ensure domain or external authentication
6. Ensure system is hardened
7. Optional: Use SSO services
8. Optional: Use centralized authorization policies

Authentication – MarkLogic Application Users

1. Configure external authentication for all MarkLogic users and use strong authentication
2. Configure communication security with SSL/TLS using third party issued certificates (no self-signed certificates permitted)
3. Configure and harden MarkLogic application server and ensure that TLS 1.1 or higher is used (no SSLv3 or TLS 1.0)

Authorization – External/Host

1. Use external authorization and ensure that group membership is limited and updated
2. If using OS level groups, ensure those are limited and are updated regularly
3. Recommended: Remove unused and generic groups for both host based authorization and group authorization
4. Optional: Host systems may be included in the authorization policies as authenticated resources

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privileges and roles to limit access to resources

Auditing – External/Host

1. Ensure that auditing is enabled at the system level
2. Ensure auditing is enabled for external authentication
3. Integrate with a centralized auditing system for enforcement of policies

Auditing – MarkLogic

1. Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Enable encryption of data at the storage or disk level if available
2. Use an external KMS to manage encryption keys (requires Advanced Security option). Integrate the KMS system with enterprise wide security policy for compliance and governance

Backup Data Security

1. Ensure backup policies are in place for MarkLogic data
2. Ensure that backups are password protected and encryption is enabled using a backup encryption certificate provisioned by an external KMS
3. If data and wallet (encryption keystore) are backed up separately, ensure that they are done atomically
4. Enable encryption for backup data

Large Deployment Environments

High Security Profile in a Large Environment

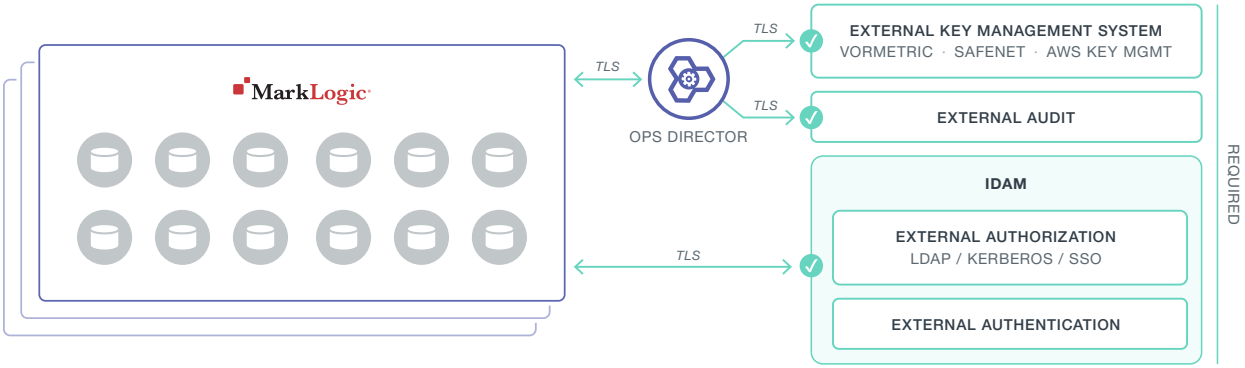


Figure 6: Architecture for a high security profile in a large environment.

Authentication – Host/System Security

1. External/Network login to be chosen for user authentication. Admin account on machine is well protected using strong credentials. Hosts must be authenticated as resources within the enterprise
2. Delete all other accounts including guest accounts
3. Ensure passwords are used. Change password on first login and establish a complex password policy along with strong authentication enforcement
4. Limit group membership on the hosts to only validated, strongly authenticated users
5. Use domain or external authentication. Use SSO services. Use centralized authorization policies
6. Ensure system is hardened

Authentication – MarkLogic Application Users

1. Configure external authentication for all MarkLogic users with strong authentication
2. Configure communication security using third party issued SSL/TLS certificates (no self-signed certificates), and use TLS 1.1 or higher (no SSLv3 or TLS 1.0)
3. Deploy and use Ops Director to manage the MarkLogic ecosystem. Ensure Ops Director is secured to a similar security profile as all other applications
4. Configure and harden MarkLogic application server

Authorization – External/Host

1. Use external authorization to ensure that group membership is limited and updated
2. If using OS level groups, ensure those are limited, restricted, and are updated
3. Remove unused and generic groups for both host based authorization and group authorization
4. Include host systems in the authorization policies as authenticated resources

Authorization – Internal/MarkLogic

1. Review and limit the roles and permissions that are defined and configured
2. Use MarkLogic's granular privilege feature to limit access to resources

Auditing – External/Host

1. Ensure that auditing is enabled at the system level
2. Ensure auditing is enabled for external authentication
3. Integrate with a centralized auditing system for enforcement of policies and compliance

Auditing – MarkLogic

1. Ensure that appropriate auditing events are enabled in MarkLogic

At-Rest Data Security

1. Enable encryption of data at the storage or disk level if available
2. Use an external KMS to manage encryption keys (requires Advanced Security option)
3. Integrate the KMS system with enterprise wide security policy for compliance and governance

Backup Data Security

1. Ensure secure backup policies are in place for MarkLogic data
2. Ensure that backups are password protected and encryption is enabled using backup encryption certificate provisioned by an external KMS
3. If data and wallet are backed up separately, ensure that they are done atomically
4. Enable encryption for backup data

HA/DR Site Availability

1. The HA/DR site must enforce all security policies deployed in the primary site. Note that KMS systems failover to other KMS systems in the same zone. Cluster hosts can failover to other hosts in the same cluster or other clusters in other zones.

Extra Large Environments

High Security Profile in an Extra Large Environment

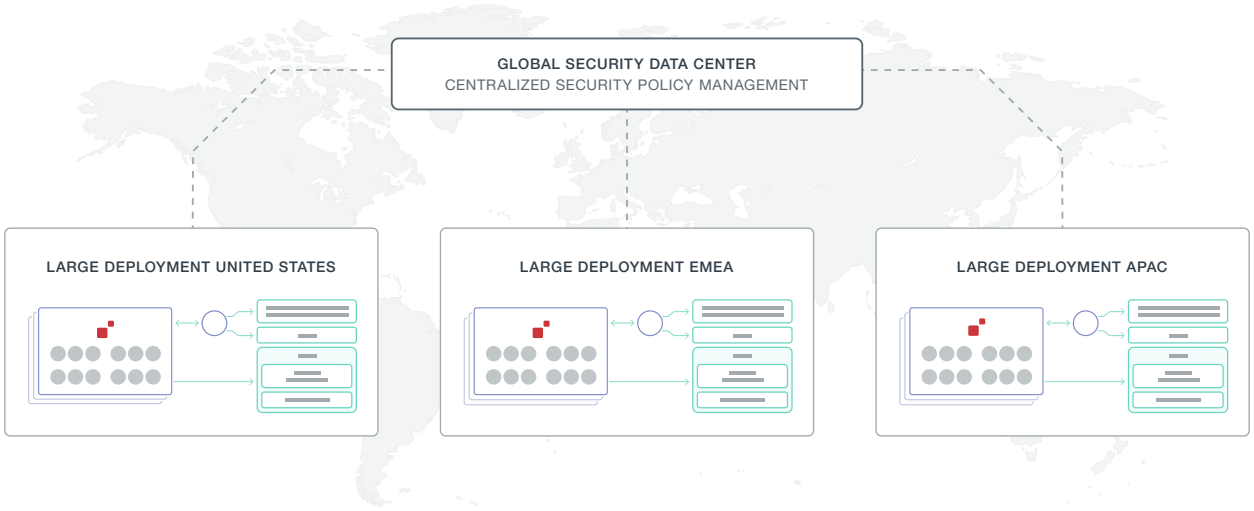


Figure 7: Architecture for a high security profile in an extra large deployment.

The checklist for extra large environments is the same as the one for a high security profile in a large environment (please refer to previous section). The only difference with an extra large environment is that now the checklist must be repeated across each geographical location.

Available Assistance

Documentation

MarkLogic provides guidance and support to enable organizations to effectively leverage existing customer infrastructure and security best practices in order to deploy a secure data environment based on MarkLogic.

Access the Security Guide at https://docs.marklogic.com/guide/security/. As part of the documentation there are **Security Recipes** that provide step-by-step instructions on how to properly implement security.

Training

Free training is available for application developers, database administrators, and system administrators through classes delivered online (at globally convenient times) from MarkLogic University.

Go to https://www.marklogic.com/training/ to register for on-demand and instructor-led training.

Support

Customers bet their business on MarkLogic, so MarkLogic Support is available for customers 24x7 with timely help available from knowledgeable support engineers.

The MarkLogic global support organization can follow the sun to work urgent issues until they are resolved. And, with the backing of MarkLogic product development and professional services organizations, MarkLogic provides holistic solutions to ensure customer long-term success.

See https://www.marklogic.com/services/support/ for more information.

How to Contact Support

Once registered as a support contact, you can contact MarkLogic Technical Support via:

- Email – support@marklogic.com
- Web – https://help.marklogic.com
- Phone – 1-855-882-8323

We recommend that all support requests be submitted via either email or web, to enhance the process of reporting, tracking and resolving issues. Support requests for urgent issues should be submitted at any time via email to urgent@marklogic.com.

Consulting Services

MarkLogic Consulting Services provides recommendations based on best practices developed from over a decade of experience deploying the most demanding, mission-critical systems. MarkLogic Consulting is very familiar with the *MarkLogic Security Model* and will work with you to guide your deployment.

See https://www.marklogic.com/services/consulting-services/ for more information.

Conclusion

In this white paper, we provided an overview of secure architectures for MarkLogic deployments. We discussed different scenarios depending on size and security profiles based on actual MarkLogic implementations and over a decade of experience.

Additional white papers, linked to below, are intended to answer additional questions for developers building applications and for security and business professionals interested in learning how we build security into the product itself.

Lastly, it is worth noting again that data security is a constantly evolving topic. This white paper is only a general guide on how to deploy MarkLogic securely. You should always refer to the documentation and MarkLogic support team for the most up to date information.

Key Resources

MarkLogic Concepts Guide on Security
https://docs.marklogic.com/guide/concepts/security

Understanding and Using Security Guide
https://docs.marklogic.com/guide/security

White Paper – Building Security Into MarkLogic
https://www.marklogic.com/resources/building-security-marklogic/

White Paper – Developing Secure Applications on MarkLogic
https://www.marklogic.com/resources/developing-secure-apps-marklogic/

999 Skyway Road, Suite 200 San Carlos, CA 94070
+1 650 655 2300 | +1 877 992 8885
www.marklogic.com | sales@marklogic.com