Application Architecture NextLabs

Status	Approved
Owner	MUTHUSAMY-ext, Kunalan
Stakeholders	Douglas de la Cruz, Milene Zeni, Domenico Cichella
LeanIX Link	NextLabs-DAE, NextLabs-DAM

- Key Decisions and Requirement
- Application Architecture
  - Overview
  - Application Components
    - NextLabs Components
    - Integrating Systems
  - NextLabs Data and Security Flow
    - NextLabs Initial Configurations
    - Encryption
    - Accessing Sensitive Data
- System Landscape
- Hosting Details
  - URL Naming Convention
    - URLs
  - Database
  - Development
  - QAS
  - Production and Parallel Run
- Application Security
  - User Access
  - Authentication
  - Communication Security
  - Data Security
  - Other Controls
- Operation Architecture
  - Change and Configuration Management
  - Monitoring
  - Sizing & Capacity Management
  - High Availability & Disaster Recovery
  - Backup
    - Backup Storage Locations
  - Maintenance Plan
- See also
- Change log

The purpose of this document is to describe the architecture of NextLabs application.

Out of Scope:

- NextLabs policy design and details will covered in a separate deliverable.
- Information related to product documentation that can be found online will not be documented here.
- NextLabs security and policy design. Please refer to NextLabs Policy Design document for details.

Key Decisions and Requirement

Description	Rationale
NextLabs will be deployed in the same Azure region as S/4HANA	Since NextLabs makes real-time decisions on access, low latency network connection will be required between S/4HANA and NextLabs to prevent performance issues.
Shared file system between S/4HANA App server and Policy controller	Azure Files from NextLabs Azure tenant will be leveraged and this file system will be used to host NextLabs DAE binaries and logs from S/4HANA
Shared file system between NextLabs Policy Controller and ICENET VMs	Azure Files will be leveraged and this file system will be used to host Policy controller logs from Policy Controller.
Azure SQL Database (DaaS) will be leveraged for NextLabs	Azure SQL Database will be leveraged to reduce operational overhead.
Sensitive data will be protected using Format-Preserving Encryption (FPE).	FPE allows Syensqo to meet export controls such as ITAR, EAR, or various UK/European Regulations.

NextLabs built-in KMS will be leveraged	For ease of integration, the NextLabs built-in KMS will be used to manage encryption keys.[1]
NextLabs policy should take user's location into consideration when evaluating access to sensitive data.	Ensures that the sensitive data is not being accessed outside the permitted country and allows Syensqo to meet export controls.
Single Sign-On (SSO)	As part of SyWay project, a common authentication mechanism (e.g., SAML) is adopted for ease of access and unified user experience.
Users must access NextLabs using HTTPS.	As part of SyWay standards, all data in transit must be encrypted.

1 NextLabs built-in KMS has limited features (e.g., Key Encryption Keys is currently not supported) and if it does not meet requirements, Voltage KMS might be used instead.

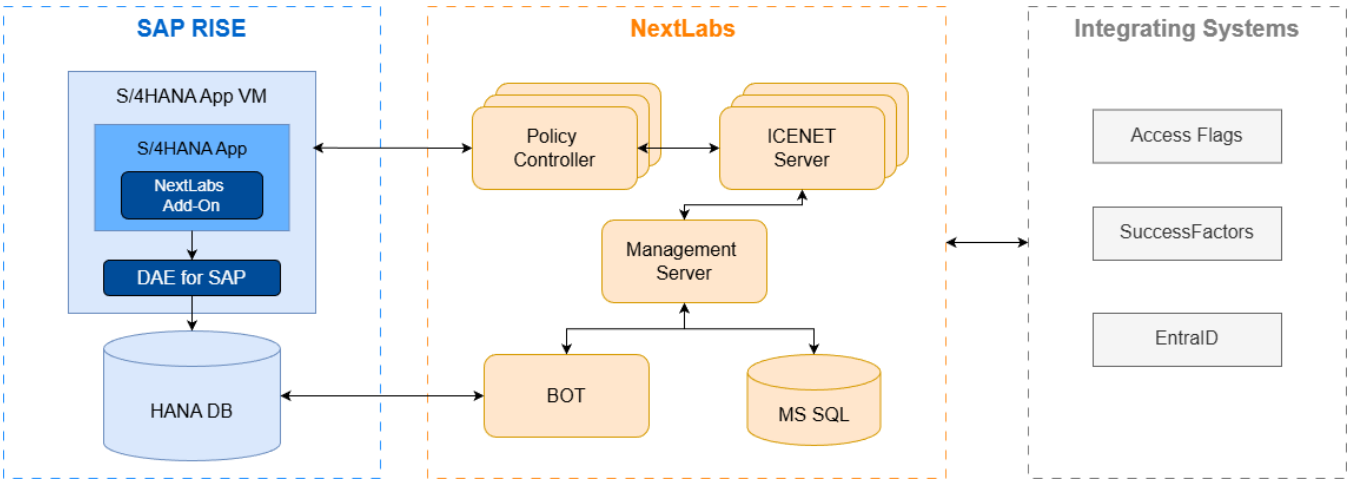
Application Architecture

Overview

Data Access Enforcer (DAE) from NextLabs will be deployed for SyWay. DAE provides fine-grained, attribute-based access control (ABAC) for data, ensuring that only authorized users or applications can access sensitive data based on real-time policies and contextual information. For SyWay, it enforces authorization decisions to grant access and decrypt sensitive data.

NextLabs Dynamic Authorization Management (DAM) extends native role-based authorization and enforces finer-grained, attribute-based controls to critical SAP applications. However, DAM can only be implemented on the SAPGUI UI level to mask data and since SyWay will be using Fiori, DAM does not fit and will not be implemented.

The following diagram describes the different NexLabs components.



Application Components

NextLabs Components

- **Policy Controller**: Key component of NextLabs that evaluate data access request against the policies and makes the decisions to deny or allow access to sensitive data.
- **ICENET Servers**: Distributes policy definitions from Management Server to Policy Controller and also clears the logs from the policy controllers by moving them to NextLabs's DB (MS SQL).
- **Management Server**: Administrative component that is used to manage NextLabs instances and policies. It is also used configure policies.
- **Bulk Obfuscation Tool (BOT):** Allows users to select which data to encrypt. In addition to encrypting data, it also creates encryption keys, stores them in NextLabs DB and writes the key ID in into a /NXL/ table in HANA DB.
- **MS SQL**: Database for NextLabs. It stores configuration, policies, logs and encryption keys used for Format-Preserving Encryption (FPE). For NextLabs Azure SQL DB (DaaS) will be leveraged.
- **DAE for SAP** : NextLabs binaries that run on SAP application. At run-time, DAE for SAP will intercept data request for sensitive request and send it to Policy controller to evaluate if access should be granted.
- **NextLabs add-on**: Installs NextLabs programs and tables in S/4HANA application.
- **Azure Files**: Network files systems are required between DAE for SAP & Policy Controller and ICENET servers & Management Servers.

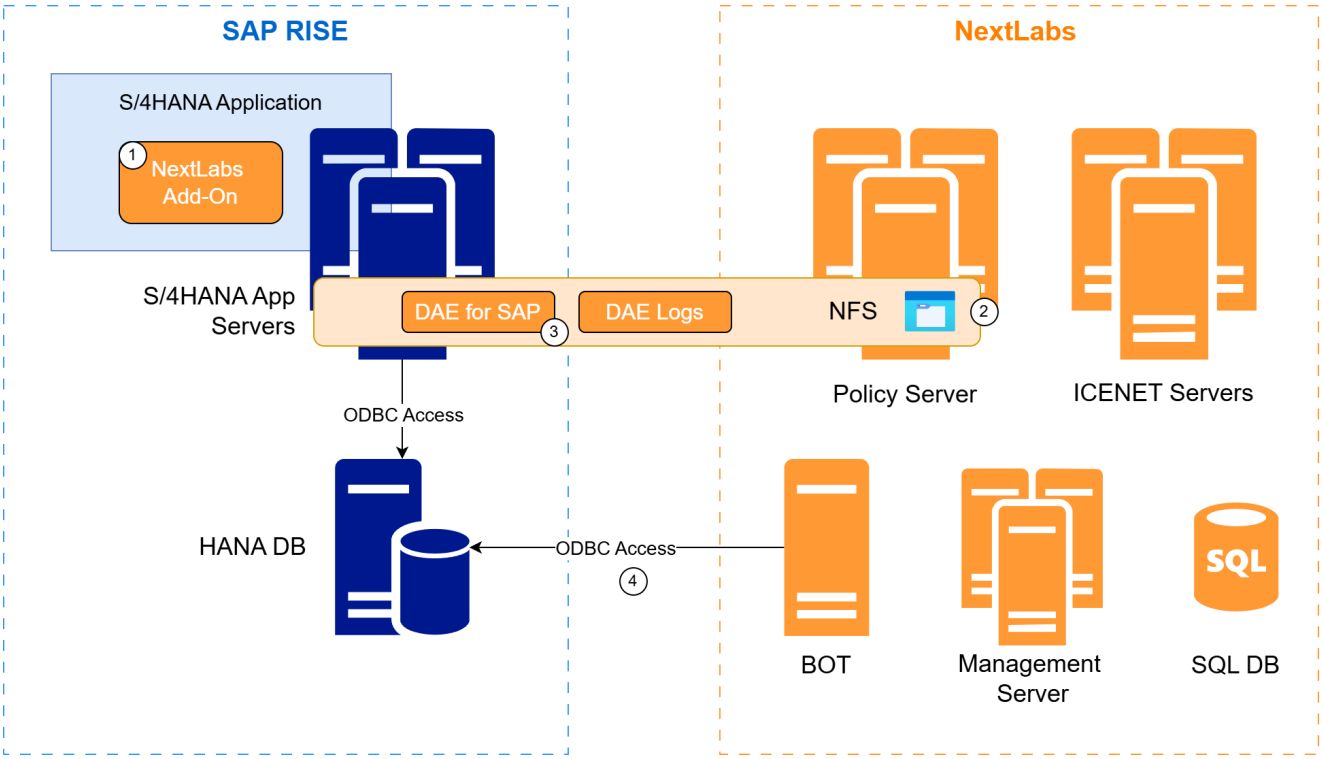
Integrating Systems

- **Access Flag**: Houses information on user access to the corresponding controlled document, taking into account the constraints from the various Export control regulations: ITAR, EAR, European Dual Use, German military.

- **SuccessFactors**: Syensqo HR system that serves as a source of truth for employee data.
- **EntraID**: Integrated with NexLabs for SAML SSO and provides the user's location at the point of SSO for access evaluation.

NextLabs Data and Security Flow

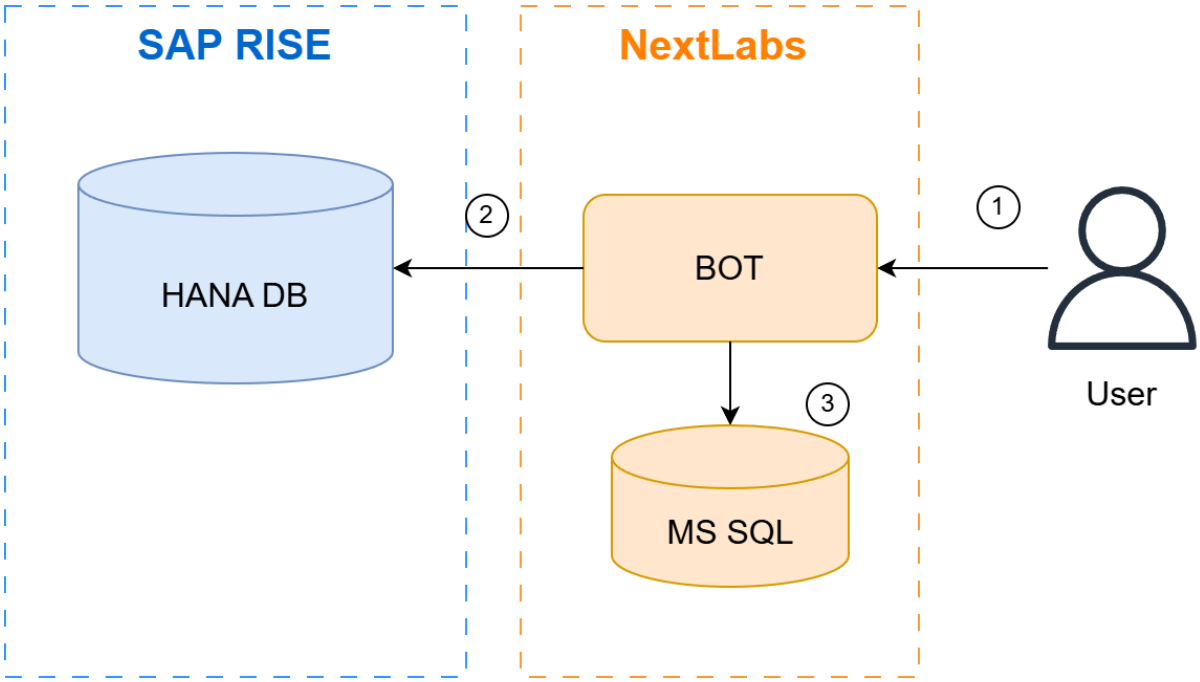
NextLabs Initial Configurations



The following steps will be carried out to prepare S/4HANA

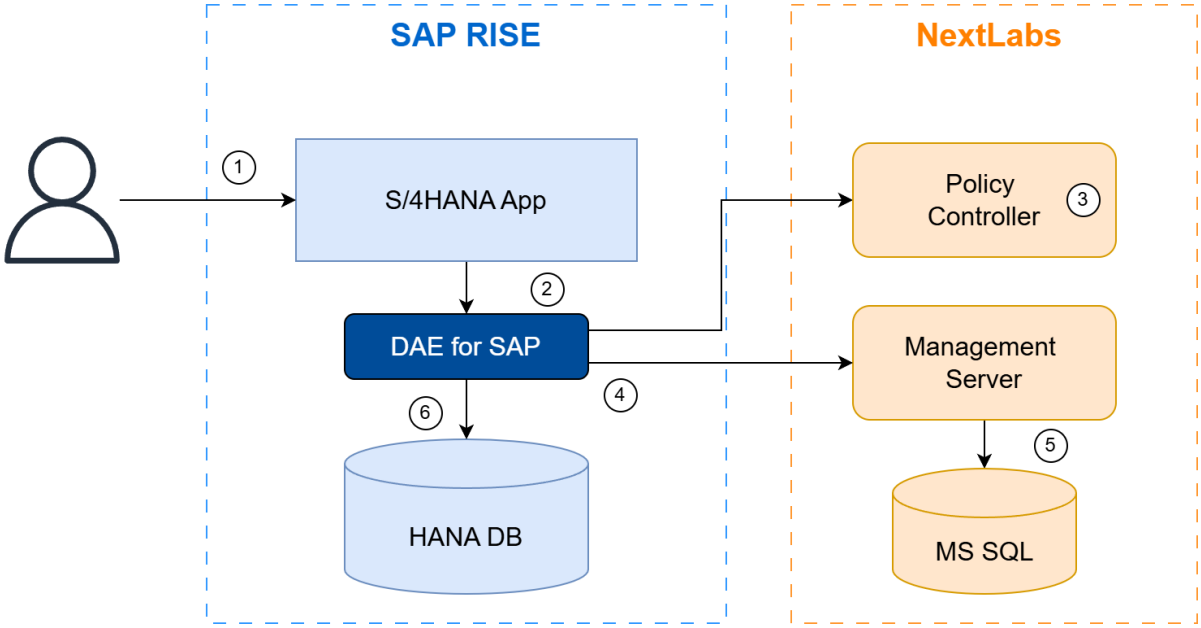
1. NextLabs add-on will be installed in S/4HANA. This will import NextLabs programs and tables in /NXL/ namespace.
2. A share file system will be mounted across S/4HANA application VMs and Policy Server VMs. This NFS will contain binaries for DAE for SAP and used to store log files from DAE.
    - Path for DAE installation - /usr/NextLabs/DAE
    - Path for DAE working and log directory - /usr/sap/<SID>/DAE
3. DAE bootstrap command is to be executed on S/4HANA application server which will load NextLabs configurations into S/4HANA Kernel. Thi s step is to be repeated when S/4HANA kernel is updated.
4. BOT component will required ODBC connection to S/4HANA.

Encryption



1. User selects which data to encrypt in BOT Web UI.
2. BOT creates an encryption key for the selected data, encrypts the data and writes the key ID in into a /NXL/ table in HANA DB.
3. BOT stores the encryption key and key ID in MS SQL DB.

Accessing Sensitive Data



Reading Sensitive Data

1. Sensitive data access is requested using any access method (SAPGUI, Fiori, interfaces etc.).
2. DAE intercepts the DB call and send the request to the Policy controller.
3. Policy controller evaluates if access should be granted based on the policies defined in NextLabs.
4. If access is granted, DAE for SAP will retrieve the encryption key ID from /NXL/ table and query Management server for the encryption key.
5. Management server retrieves the key from MS SQL DB and sends it to DAE.
6. DAE reads the encrypted data from HANA DB, decrypts the data and returns the decrypted data to SAP application.

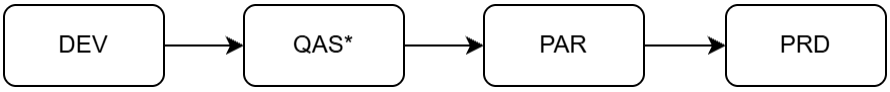
Writing Sensitive Data

1. User or interface tries to update S/4HANA Data from web or SAPGUI.
2. DAE for SAP intercepts the DB write command and sends it to Policy Controller.

3. Policy Controller evaluates if the write command contains sensitive data and the users has access to the corresponding data.
4. If yes, DAE for SAP will retrieve the encryption key ID from /NXL/ table and query Management server for the encryption key.
5. Management server retrieves the key from MS SQL DB and sends it to DAE.
6. DAE for SAP uses the encryption key to replace the sensitive data in the write command with its corresponding encryption value and send the write command to HANA DB.

System Landscape

NextLabs landscape will consist of a 4-tier landscape.



*QAS instance will be integrated to INT and UAT landscapes.

Hosting Details

NextLabs system will be hosted in both EU and US region. Since NextLabs requires low latency network connection to S/4HANA, NextLabs will be hosted in the same Azure region and physical zone as SAP RISE.

Region	Azure Region
EU	North Europe (Dublin)

In EU and US, NextLabs will be deployed to the following Subscriptions and vNETs. In both regions, NextLabs vNETs will be attached to region's Syensqo's Hub. To optimize latency between S/4HANA and NextLabs, NextLabs will be deployed in the same zone as SAP RISE.

Region	Subscriptions	vNET	Azure physicalZone
EU	Non-PRD	DEV	northeurope-az1
		QAS	northeurope-az1
	Pre-PRD	PAR	northeurope-az1 northeurope-az3
	PRD	PRD	

For more details on NextLabs infrastructure please refer to Network and Infrastructure Architecture .

URL Naming Convention

NextLabs Policy Controller, ICNET and Management server components require an FQDN to be defined. The following URL naming convention will be adopted.

Component URL*:* NXL-<environment>-<component><##>.syensqo.com

Load balancer URL*:* *NXL-<environment>-<component>.syensqo.com*

Parameter	Values
environment	• dev, qas, par • For production this parameter will be omitted.
component	• Java Policy Controller - jpc • ICENET - icenet • Control Center - cc
XX	• 01, 02 (in running sequence based on the number of instances.

URLs

Environment	Component	URL
	Control Center	https://nxl-dev-cc.syensqo.com

DEV	Policy Validator	https://nxl-dev-cc.syensqo.com:6443
	Java Policy Controller	https://nxl-dev-jpc01.syensqo.com:8443

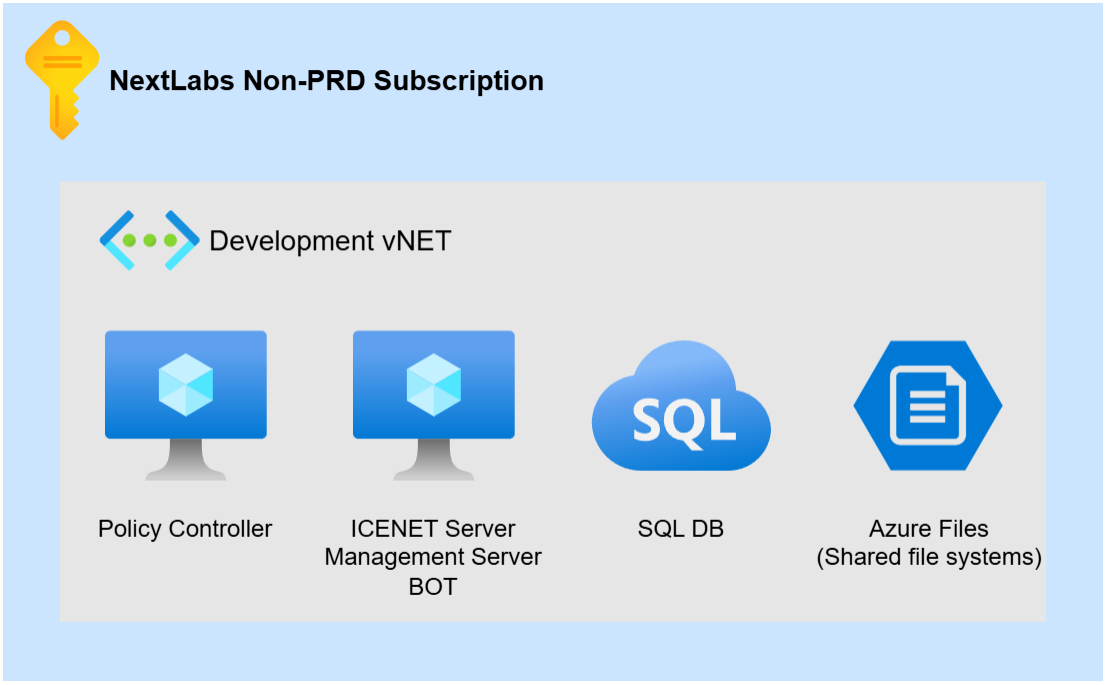
Database

Azure SQL Server (DaaS) service will be used as NextLabs database. The table below summaries the DB details

Environment	SQL Server	SQL DB	IP	Schema	DB User	DB Link
DEV	azrneuvmldnlaapp0000	azrneusdbdnlasha0000	172.16.48.20	dbo	dev_ccdbuser	Link

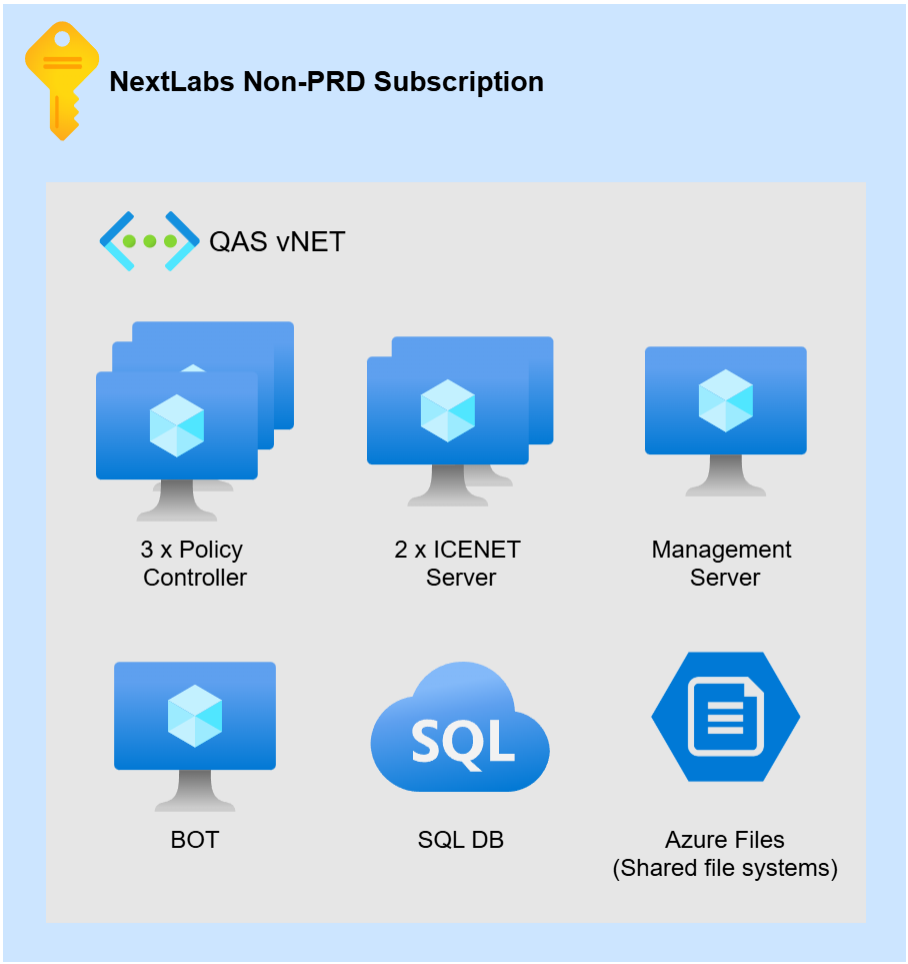
Development

Development NextLabs instance will follow combined deployment where multiple components are deployed together.



QAS

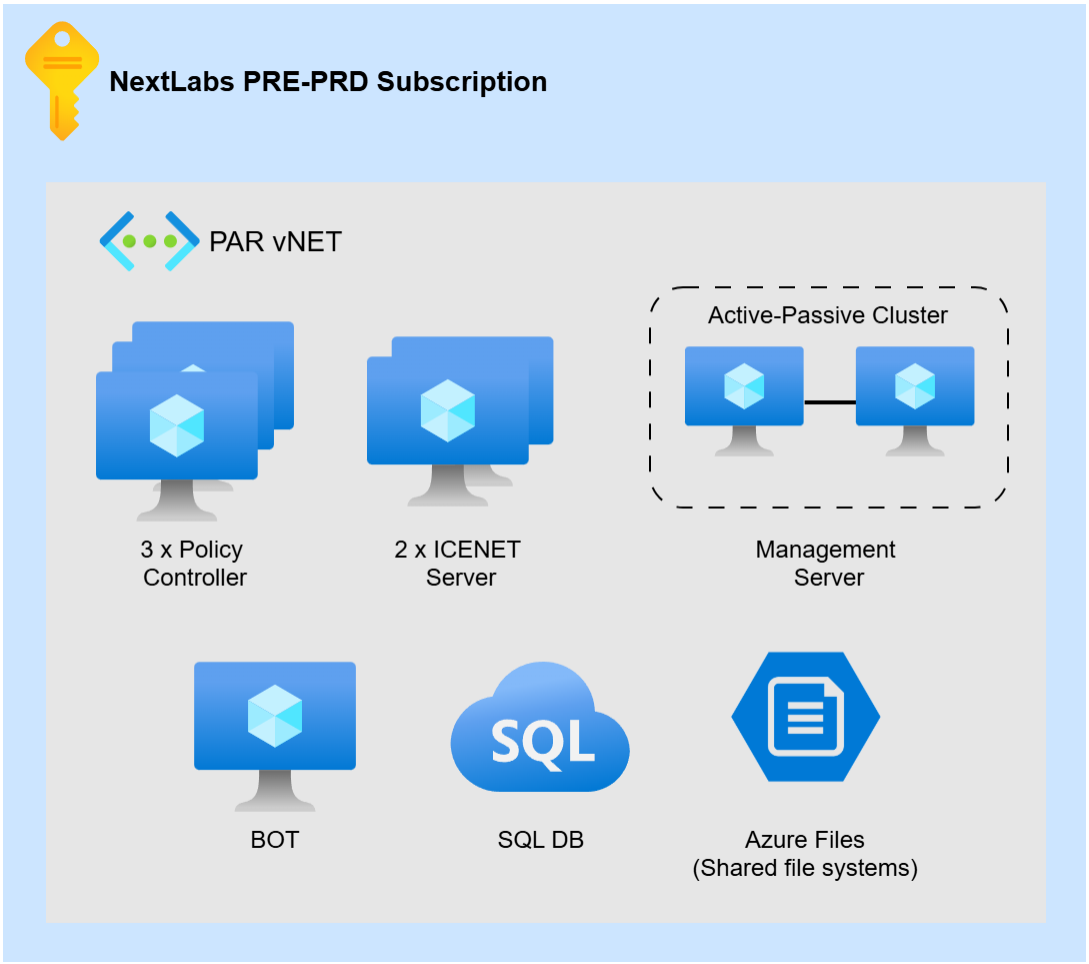
QAS NextLabs instance will follow a distributed deployment with no high-availability (HA).



Production and Parallel Run

Parallel run instance will follow a high-availability architecture.

- Multiple instances of Policy controller and ICENET servers will be deployed in an active-active configuration.
- Management server will be deployed in an active-passive configuration using RHEL Pacemaker.
- Azure built-in high-availability will be leveraged for SQL DB and Azure Files.
- Since BOT is not runtime critical, it will be deployed without HA.



Application Security

User Access

NextLabs will be accessed by NextLabs administrators from Syensqo network via HTTPS. Default security roles will be used.

Authentication

NextLabs is configured to perform SAML SSO with Syensqo Entra ID.

Communication Security

Data in transit is encrypted using secure TLS protocols (v.1.2 or greater) with 2048-bit keys.

Data Security

The following controls are implemented to ensure data security:

- Encryption is enable to protect data at rest
  - Transparent Data Encryption (TDE) will be enabled for Azure SQL Database.
  - As part of Syensqo's standard disk encryption is enabled by default.
  - All backup are encrypted.
  - As part of Syensqo's Azure standards, encryption keys must be customer managed and is stored in the respective KMS provisioned for each environment.
- Data protection.
  - All backups are storage in immutable storage.
  - Non-PRD backups are stored in zone redundant storage.
  - Production backups are stored in Geo-redundant storage and are replicated to another region.

Other Controls

- The target availability SLA for NexLabs is 99.95% (similar to S/4HANA).
- CrowdStrike endpoints installed on VMs.

Operation Architecture

Change and Configuration Management

NextLabs policies will be transported using NextLabs Policy Migration tool. This tool will be configured to transport to DEV QAS PAR PRD.

Monitoring

The following monitoring will be enabled for NextLabs.

Type	Metrics monitored	Alerts Trigger	Monitoring Tool
VM Availability	VM is running	VM status is not available	*TBC*
High resource utilization	CPU	CPU utilization > 85%	*TBC*
	Memory	Memory utilization > 85%	*TBC*
	Disk	Disk utilization > 85%	*TBC*
OS Services	NextLab services	Services are down	*TBC*
Backup	Backup status	Backup status is not successful	*TBC*

Sizing & Capacity Management

TBC

High Availability & Disaster Recovery

NextLabs HA/DR approach is similar to S/4HANA - Short distance disaster recovery. With this approach, Redundant NextLabs components will be deployed across 2 zones.

The following table lists down the HA/DR approach for each component.

Component	HA Design
Policy Controller	Multiple Policy Controller VMs will be deployed across 2 AZ in an active-active configuration.
ICENET Servers	Multiple ICENET Servers will be deployed across 2 AZ in an active-active configuration.
Management Server	2 Management Server VMs will be deployed across 2 AZ in an active-passive configuration and RHEL Pacemaker will be leveraged to manage the failover.
Bulk Obfuscation Tool (BOT)	BOT is not critical to runtime. Hence one instance of BOT will be deployed.
MS SQL	SQL managed instance (DaaS) will be used for NextLabs and HA is provided by Microsoft.
Azure Files (DAE for SAP)	Azure Files built-in HA capabilities will be leveraged.

For more details please refer to DD-TEC-140 HA/DR Architecture Design.

Backup

The following backups are configured for NextLabs.

Tier	Backup Type	Frequency
DEV & QAS	VM	Weekly
	Azure File	Daily
	DB	Daily

Pre-PRD & PRD	VM	Weekly
	Azure File	Daily
	DB	Daily
	DB log	Hourly

For more details please refer to DD-TEC-160 Back up and Restore Design.

Backup Storage Locations

TBC

Maintenance Plan

Syensqo's maintenance and patching schedule will be adopted for NextLabs systems.

For parallel run and production instance, the HA configuration will be leverage to perform the activities without downtime.

See also

- LeanIX Factsheet - NextLabs-DAE

Change log

Version	Published	Changed By	Comment
CURRENT (v. 43)	**Mar 18, 2026 09:16**	**MUTHUSAMY-ext, Kunalan**	
v. 42	Mar 17, 2026 10:09	**MUTHUSAMY-ext, Kunalan**	
v. 41	Mar 17, 2026 09:34	**WENNINGER-ext, Sascha**	
v. 40	Mar 17, 2026 08:58	**MUTHUSAMY-ext, Kunalan**	
v. 39	Mar 11, 2026 09:55	**MUTHUSAMY-ext, Kunalan**	
v. 38	Mar 11, 2026 09:41	**WENNINGER-ext, Sascha**	added stakeholders
v. 37	Feb 24, 2026 08:01	**MUTHUSAMY-ext, Kunalan**	
v. 36	Feb 04, 2026 08:04	**MUTHUSAMY-ext, Kunalan**	
v. 35	Jan 21, 2026 05:10	**MUTHUSAMY-ext, Kunalan**	
v. 34	Jan 12, 2026 06:45	**MUTHUSAMY-ext, Kunalan**	

Go to Page History

Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

Mar 30, 2026	Actor	Type	Activity	Version
Approved	WENNINGER-ext, Sascha	State	changed state to Approved at 8:01 am	v43
Pending SteerCo Review	WENNINGER-ext, Sascha	State	gave *Final Approval* approval at 8:01 am *Approved by Frank Bolata. Email attached*	

Mar 23, 2026

	WENNINGER-ext, Sascha	State	changed expiry date to '06 Apr, 2026 02:56 pm' at 3:56 pm	
		State	changed state to Pending SteerCo Review at 3:56 pm	v43
Pending Stakeholder Review	WENNINGER-ext, Sascha	State	gave *Stakeholder Review* approval at 3:56 pm *All open comments were addressed and accepted, emails attached.*	
		State	changed expiry date to '30 Mar, 2026 02:56 pm' at 3:56 pm	
		State	changed state to Pending Stakeholder Review at 3:56 pm	v43
Edited following DA Endorsement	WENNINGER-ext, Sascha	State	gave *Minor change* approval at 3:56 pm *updates following stakeholder review*	