



第三方元件檢測及管理系統建置案 Sonatype Nexus Repository 管理者教育訓練

精誠資訊

大綱

- 軟體簡介
- 存取控制
- 通知管理
- Firewall阻擋與Waive機制
- 管理自行開發套件

The background features a vibrant blue color palette. On the left side, there is a large, light blue circle. Overlapping this circle is a darker blue circle, which in turn contains a light greenish-blue circle. A dark blue spiral starts from the center of these circles and winds outwards towards the bottom left. The right side of the image is a solid, medium blue.

Sonatype軟體簡介

Sonatype Platform



- Sonatype Lifecycle

- 自動檢測和提供修復建議，在DevOps中實踐安全開發並避免攻擊。

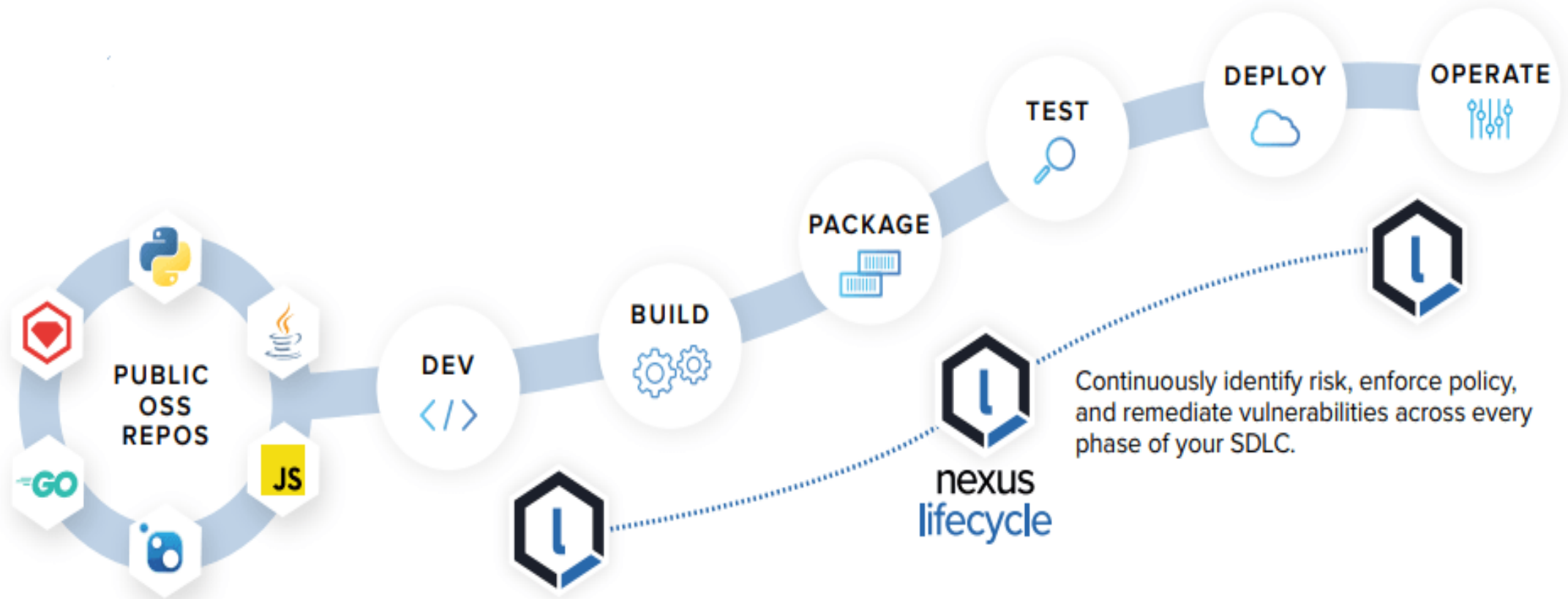
- Sonatype Nexus Repository

- 提供單一安全套件來源；支援多達18種主流套件儲存庫。

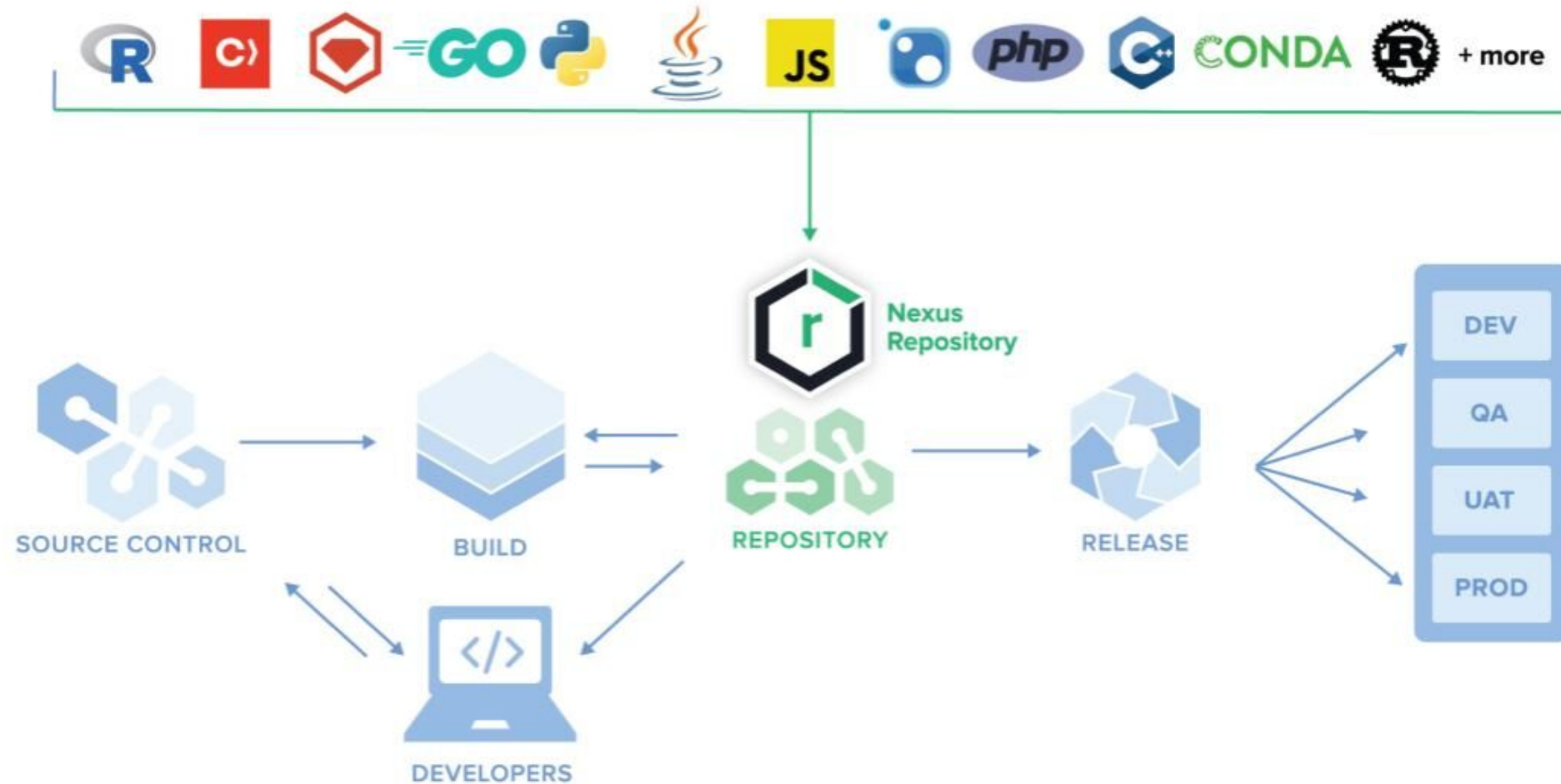
- Sonatype Repository Firewall

- 早期識別和預警，自動阻止已知漏洞和有害的套件版本以降低風險。

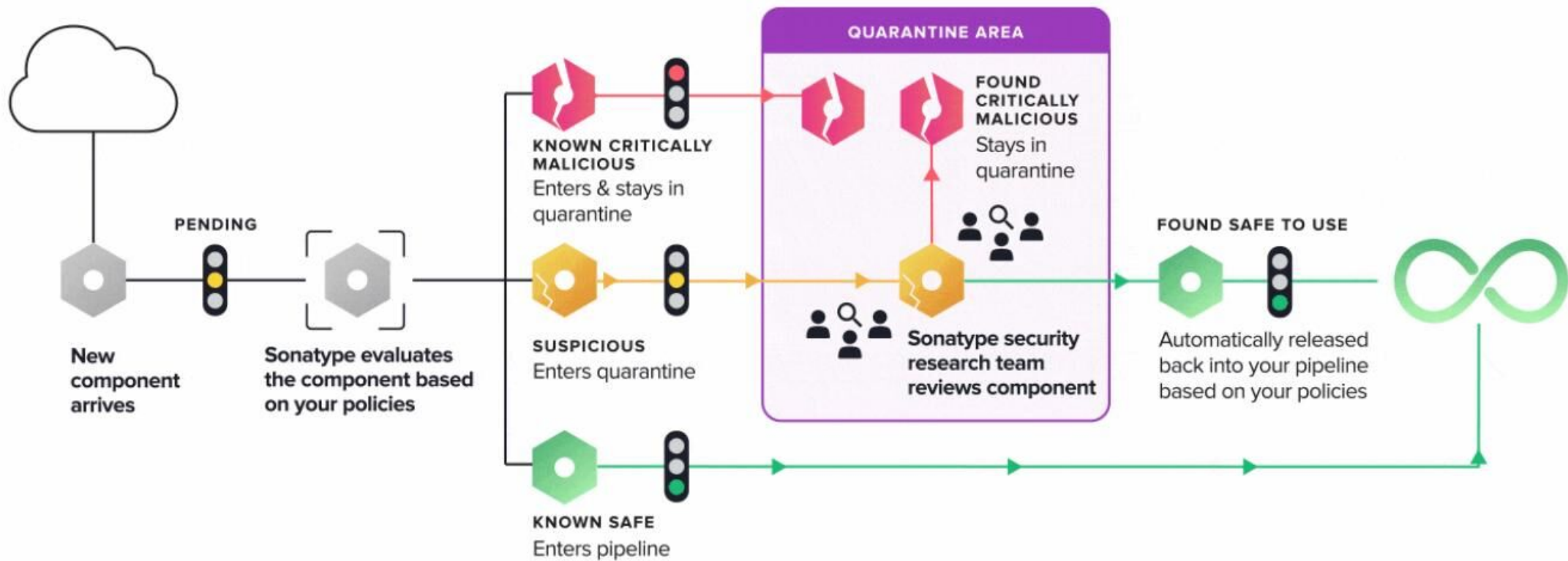
Sonatype Lifecycle



Sonatype Nexus Repository



Sonatype Repository Firewall



The background features a series of concentric circles and a spiral pattern in various shades of blue and teal. The spiral starts from the center and expands outwards, creating a sense of depth and movement. The colors range from a deep blue in the center to a lighter, almost white blue at the edges.

存取控制

LDAP 整合

The screenshot displays the Sonatype Nexus Repository Administration interface. The left sidebar contains the 'Administration' menu with options like Users, Anonymous Access, Atlassian Crowd, LDAP, Realms, SAML, SSL Certificates, User Tokens, IQ Server, Support, System, API, Bundles, and Capabilities. The 'LDAP' option is highlighted with a red box. The main content area shows the 'LDAP' configuration page with a red box around the 'Create connection' button. A yellow arrow points from the 'LDAP' menu item to the 'Create connection' button. Another yellow arrow points from the 'Create connection' button to the 'LDAP' menu item. The top navigation bar includes the Sonatype Nexus Repository logo, version PRO 3.70.1-02, a search bar, and a settings gear icon. The main content area also displays a table with columns 'Order', 'Name', and 'URL', and a message stating 'There are no LDAP servers defined or you don't have permission to browse them'. A section titled '? What is LDAP?' provides information about configuring authentication and user role mapping, including a link to 'documentation'.

Sonatype Nexus Repository
PRO 3.70.1-02

Administration

- Users
- Anonymous Access
- Atlassian Crowd
- LDAP**
- Realms
- SAML
- SSL Certificates
- User Tokens
- IQ Server
- Support
- System
- API
- Bundles
- Capabilities

LDAP Manage LDAP server configuration

Create connection Change order Clear cache

Order	Name	URL
-------	------	-----

There are no LDAP servers defined or you don't have permission to browse them

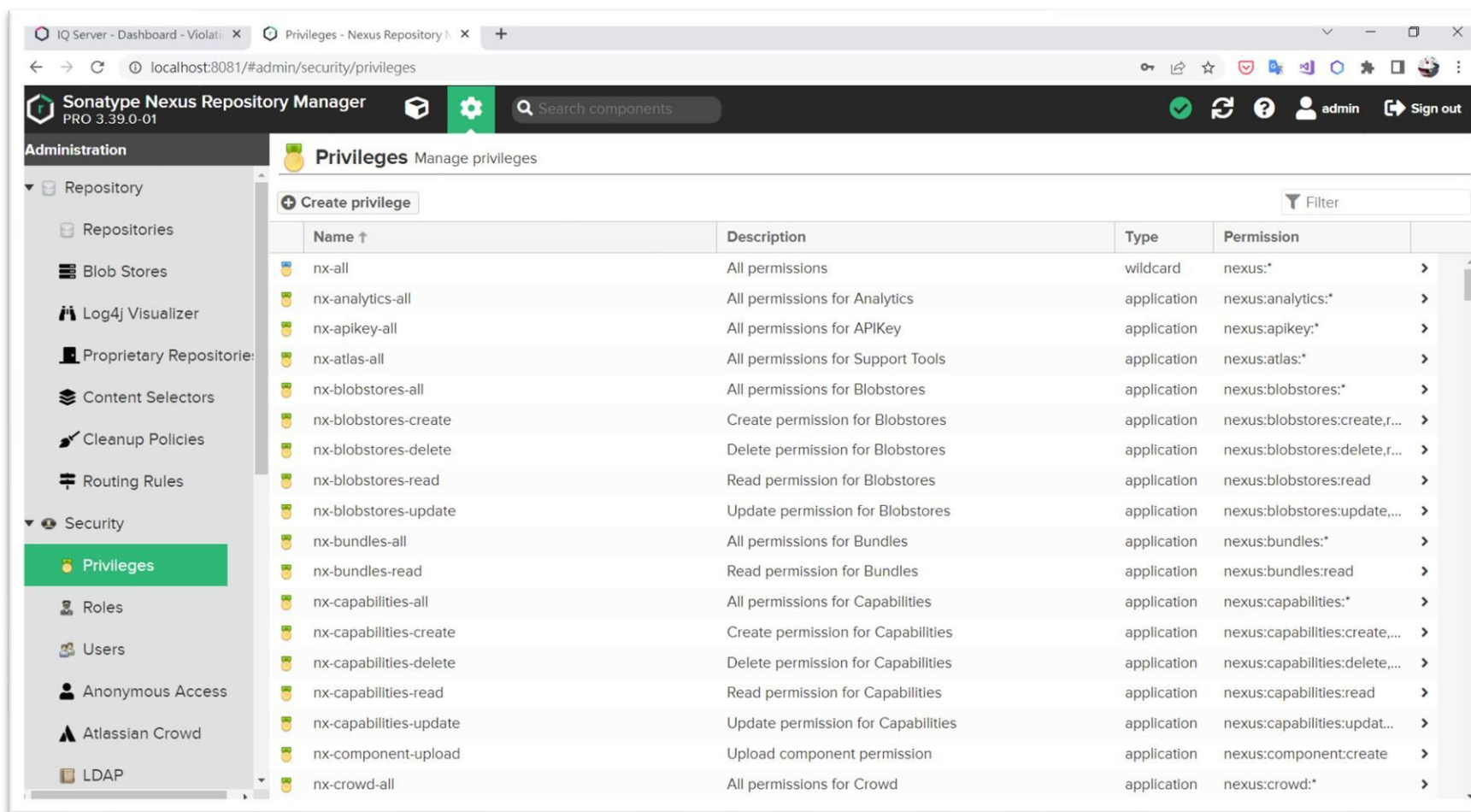
? What is LDAP?

You can configure your NXRM instance to use LDAP for authentication and user role mapping. The repository can cache authentication information and support multiple LDAP servers and user/group mappings to take advantage of central authentication set up across your organization's repository managers. For more information, see the [documentation](#).

LDAP 設定

Server Name	名稱
LDAP server address	ldap://***.***.***.***:389
Search base DN	ou=XXX,dc=YYYY,dc=corp
Authentication method	Simple Authentication
Username or DN	用於查詢LDAP的帳號
Password	*****
User relative DN	用於指定使用者的組織 例：ou=資訊部
Object class	Person
User ID attribute	sAMAccountName
Real name attribute	用於顯示使用者名稱的欄位 例：cn
Email attribute	用於帶入使用者郵件的欄位 例：mail

權限定義






The screenshot shows the Sonatype Nexus Repository Manager interface. The left sidebar contains the 'Administration' menu with 'Privileges' selected. The main content area displays a table of privileges.

Name	Description	Type	Permission
nx-all	All permissions	wildcard	nexus:*
nx-analytics-all	All permissions for Analytics	application	nexus:analytics:*
nx-apikey-all	All permissions for APIKey	application	nexus:apikey:*
nx-atlas-all	All permissions for Support Tools	application	nexus:atlas:*
nx-blobstores-all	All permissions for Blobstores	application	nexus:blobstores:*
nx-blobstores-create	Create permission for Blobstores	application	nexus:blobstores:create,r...
nx-blobstores-delete	Delete permission for Blobstores	application	nexus:blobstores:delete,r...
nx-blobstores-read	Read permission for Blobstores	application	nexus:blobstores:read
nx-blobstores-update	Update permission for Blobstores	application	nexus:blobstores:update,...
nx-bundles-all	All permissions for Bundles	application	nexus:bundles:*
nx-bundles-read	Read permission for Bundles	application	nexus:bundles:read
nx-capabilities-all	All permissions for Capabilities	application	nexus:capabilities:*
nx-capabilities-create	Create permission for Capabilities	application	nexus:capabilities:create,...
nx-capabilities-delete	Delete permission for Capabilities	application	nexus:capabilities:delete,...
nx-capabilities-read	Read permission for Capabilities	application	nexus:capabilities:read
nx-capabilities-update	Update permission for Capabilities	application	nexus:capabilities:updat...
nx-component-upload	Upload component permission	application	nexus:component:create
nx-crowd-all	All permissions for Crowd	application	nexus:crowd:*

Repository Manager 已定義一套非常詳盡的權限項目，此權限只能被設定在角色。

要擁有建立權功能的使用者，需具備 nx-privilege或是 nx-all 的權限。

角色定義

 Roles Manage roles			
<div><div><div></div></div><div>Create role</div></div>		<div><div></div><div>Filter</div></div>	
	Name ↑	Source	Description
	nx-admin	Nexus	Administrator Role >
	nx-anonymous	Nexus	Anonymous Role >

nx-admin	nx-anonymous
nx-all	nx-healthcheck-read nx-repository-view-*-*-browse nx-repository-view-*-*-read nx-search-read

預設已建立 nx-admin 及 nx-anonymous 兩個角色。

nx-admin: 提供管理者完整的權限項目。

nx-anonymous: 提供匿名使用者可搜尋及讀取儲存庫的功能。

要檢視角色定義的使用者，須擁有 nx-roles 權限。

建立角色

Role ID: 設定角色ID

Role name: 設定角色名稱

Role description: 該角色描述說明

Priviledges: 選擇將賦與的權限 (有提供過濾功能)



Roles: 選擇要使用此角色權限的其他角色 (有提供過濾功能)

要建立角色定義的使用者，須擁有 nx-roles 及 nx-priviledge-read 權限。

The screenshot shows a 'Create role' form with the following sections:

- Role ID:** A text input field with a red error message: 'This field is required'.
- Role name:** A text input field with a red error message: 'This field is required'.
- Role description:** A text input field.
- Priviledges:** A section with two columns: 'Available' and 'Given'. The 'Available' column has a filter icon and a list of privileges: nx-all, nx-analytics-all, nx-apikey-all, nx-atlas-all, nx-blobstores-all, nx-blobstores-create, nx-blobstores-delete, and nx-blobstores-read. There are right and left arrow buttons between the columns.
- Roles:** A section with two columns: 'Available' and 'Contained'. The 'Available' column has a filter icon and a list of roles: nx-admin, nx-anonymous, and Replication role. There are right and left arrow buttons between the columns.
- Buttons:** At the bottom, there are 'Create role' and 'Cancel' buttons.

使用者定義

 Users Manage users							
<div><div> Create local user</div><div>Source:  Local</div><div>Filter by user ID </div></div>							
	User ID ↑	Realm	First name	Last name	Email	Status	
	admin	default	Administrator	User	admin@example.org	active	>
	anonymous	default	Anonymous	User	anonymous@example.org	active	>

預設已建立 admin 及 anonymous 兩個使用者，分別對應 nx-admin 及 nx-anonymous 角色

要檢視使用者定義的使用者，須擁有 nx-users 權限。

建立使用者

ID:
admin

First name:
Administrator

Last name:
User

Email:
Used for notifications
admin@example.org

Status:
Active

Roles:

Available	Granted
<div>Filter</div> <div>nx-anonymous</div> <div>Replication role</div>	<div>nx-admin</div>

Save **Discard**

ID: 設定使用者ID

First name / Last name: 設定使用者名稱

Email: 該使用者郵件帳號




Status: Active 或是 Disabled

Roles: 選擇要授與此使用者的角色 (有提供過濾功能)

要建立使用者的使用者，須擁有 nx-users 及 nx-roles-read 權限。

Default Role

Repository Manager 提供了一個機制，可以為任何有登入權限的使用者，賦與指定角色的權限；應用於任何需開放給所有人一致的權限設定。例如：短期賦與所有使用者可存取某個儲存庫。

 **Capabilities** /  **Select Capability Type** /  **Create Default Role Capability**

☒ Enable this capability

Role:
The role which is automatically granted to authenticated users

nx-anonymous

Create capability

Cancel

匿名存取

The screenshot shows a web-based administration interface. On the left is a sidebar menu under the heading 'Administration' with the following items: Roles, Users, Anonymous Access (highlighted), Atlassian Crowd, LDAP, Realms, SAML, SSL Certificates, User Token, IQ Server, Support, and System. The main content area is titled 'Anonymous Access' with a subtitle 'Configure anonymous access to server contents'. It contains three sections: 'Access' with a checked checkbox 'Allow anonymous users to access the server'; 'Username' with a text input field containing 'anonymous'; and 'Realm' with a dropdown menu showing 'Local Authorizing Realm'. At the bottom right are 'Discard' and 'Save' buttons.


啟用匿名存取後，任何登入的使用者都將獲得指定 username 的權限，在預設的情況下，匿名用戶可以讀取所有套件儲存庫的內容。

您也可以指定一個在 LDAP 中的帳戶，使該帳戶作為匿名登入權限。



通知管理

通知設定 - SMTP

 **Email Server** Manage email server configuration

Enabled:
☐

Host:

Port:

Use the Nexus truststore:
☐ Use certificates stored in the Nexus truststore to connect to external systems [View certificate](#)

Username:

Password:

From address:

Subject prefix:

SSL/TLS options:
☐ Enable STARTTLS support for insecure connections
☐ Require STARTTLS support
☐ Enable SSL/TLS encryption upon connection
☐ Enable server identity check

[Save](#) [Discard](#) [Verify email server](#)

Hostname:

..***.***

Port:










25

From address:

nexus@sonatype

通知使用時機

- 可使用於 Tasks 的設定，在執行失敗時進行通知。




 Tasks Manage scheduled tasks								
 Create task		 Filter						
	Name ↑	Type	Status	Schedule	Next run	Last run	Last result	
	Cleanup service	Admin - Cleanup repositori...	Waiting	advanced	Thu Oct 06 2022 01:00:00...	Wed Oct 05 2022 09:09:4...	Ok [0s]	>
	Statistics - recalculate vuln...	Statistics - recalculate vuln...	Waiting	advanced	Thu Oct 06 2022 00:04:0...	Wed Oct 05 2022 09:09:4...	Ok [0s]	>
	System - Repository Health...	Check for new report avail...	Waiting	hourly	Wed Oct 05 2022 15:44:41 ...	Wed Oct 05 2022 10:04:17 ...	Ok [1s]	>
	System - Repository Health...	Check for new report avail...	Waiting	hourly	Wed Oct 05 2022 15:44:38...	Wed Oct 05 2022 10:04:17 ...	Ok [1s]	>
	System - Repository Health...	Check for new report avail...	Waiting	hourly	Wed Oct 05 2022 15:44:44...	Wed Oct 05 2022 10:04:17 ...	Ok [3s]	>
	System - Repository Health...	Check for new report avail...	Waiting	hourly	Wed Oct 05 2022 15:44:43...	Wed Oct 05 2022 10:04:17 ...	Ok [2s]	>



Firewall阻擋與Waive機制





Using Audit and Quarantine

- Audit and Quarantine 功能可以保護您的開發環境，避免受到有風險的不良套件影響。這個功能使用 IQ Server 的 Policy 管理機制來識別，並在符合條件時阻止套件進入儲存庫。
- Audit and Quarantine 功能使用位於 Root Organization 的 Policy 政策，依其中的 Actions 在 Proxy 的 Fail 設定，對符合其條件的套件進行阻擋。







ACTIONS							
ACTION	PROXY	DEVELOP	SOURCE	BUILD	STAGE	RELEASE	OPERATE
No Action	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
 Warn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
 Fail	<input checked="" type="radio"/> 	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Setting Capabilities

- 透過在 Repository Manager 中，設定 System > Capabilities 中的 IQ: Audit and Quarantine 項目，指定將受 Firewall 限制的儲存庫項目，即可為該儲存庫啟用 Policy 阻擋功能。

 Capabilities Manage capabilities					
+ Create capability			<input type="text" value="Filter"/>		
	Type ↑	Category	Description	Notes	
	Audit	Audit	Enabled	Automatically added on...	>
	Health Check: Configur...	Health Check	Configured for all supp...	⊘	>
	IQ: Audit and Quarantine	IQ	maven-a	⊘	>
	IQ: Server Configuration	IQ	⊘	⊘	>


Viewing Repository Result

Browse Browse assets and components							
	Name ↑	Type	Format	Status	URL	Health check	IQ Policy Violati...
	maven-a	proxy	maven2	Online - Ready to Connect	 copy	 40  8	11  4  >

- 在 IQ: Audit and Quarantine 機制啟用後，當有套件被阻擋下來時，可由 Browse 功能看到被隔離的套件數量，透過連結可查詢套件的詳細資訊。

Repository results for *maven-a*

Oldest evaluation 6 days ago



**80**
COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE IDENTIFIED

11
POLICY ALERTS
AFFECTING 11 COMPONENTS

4
QUARANTINED COMPONENTS

FILTER: All Exact Unknown

VIOLATIONS: Summary All Quarantined Waived

Policy Threat ▾	Component ▴	Quarantined
<input type="text" value="Search Name"/>	<input type="text" value="Search Coordinates"/>	
Security-Critical	 com.thoughtworks.xstream : xstream : 1.4.5	

Waivers with Firewall

FILTER: All Exact Unknown **VIOLATIONS:** Summary All Quarantined Waived

Policy Threat **Component** **Quarantined**

Search Name Search Coordinates

Security-Critical com.thoughtworks.xstream : xstream : 1.4.5

Component Info **Policy** Licenses Vulnerabilities Labels

Quarantined Release Quarantine View Existing Waivers

Security-High	High risk CVSS score	Found security vulnerability CVE-2021-21348 with severity >= 7 (severity = 7.5) Found security vulnerability CVE-2021-21348 with severity < 9 (severity = 7.5)	Waive
Security-High	High risk CVSS score	Found security vulnerability CVE-2021-21349 with severity >= 7 (severity = 8.6) Found security vulnerability CVE-2021-21349 with severity < 9 (severity = 8.6)	Waive
Security-High	High risk CVSS score	Found security vulnerability CVE-2021-43859 with severity >= 7 (severity = 7.5) Found security vulnerability CVE-2021-43859 with severity < 9 (severity = 7.5)	Waive

Security-High com.thoughtworks.xstream : xstream : 1.4.5

Showing all 37 rows

此處會列出導致隔離的每一項 policy，在確認接受此風險時，可以點選 Waive 來進行解除隔離。

Add Waiver

Add Waiver

Policy

Security-Critical

Constraint Name

Critical risk CVSS score

Conditions

Found security vulnerability CVE-2013-7285 with severity >= 9 (severity = 9.8)

Scope

☐ This violation only

☒ Scoped Waiver

Scope

Repository - maven-a

Component

☒ com.thoughtworks.xstream : xstream : 1.4.5

☐ All components

Comments

Scope:

This violation only: 僅針對指定的 policy 進行解除，若違反一項以上的 policy，須逐項檢討是否解除其違規風險。

Scoped Waiver: 可針對指定的儲存庫，或是 repository manager 下的所有儲存庫，解除指定的套件阻擋，或是解除所有違反此 policy 的阻擋條件。



管理自行開發套件

上傳自建的套件

Browse

Welcome

Search

Browse

Tags

Upload

[IQ Server Dashboard](#)

Upload

Upload content to the hosted repository

Filter

NAME	FORMAT	URL
maven-releases	maven2	>
nuget-hosted	nuget	>
pypi-hosted	pypi	>
raw-hosted	raw	>

上傳Maven格式的套件

Upload

Upload content to the hosted repository

* Required fields are marked with an asterisk.

Choose Assets/Components for maven-releases Repository

File *

Choose File

No file selected

Classifier

Extension *

+ Add another asset

Component coordinates

Group ID *


Artifact ID *

Version *

☐ Generate a POM file with these coordinates

Packaging

上傳其他格式的套件

 **Upload**

Upload content to the hosted repository

*** Required fields are marked with an asterisk.**

Choose Assets/Components for nuget-hosted Repository

File *

Choose File

No file selected

Component attributes

Tag

Cancel

Upload

上傳任意二進位檔案

Upload

Upload content to the hosted repository

* Required fields are marked with an asterisk.

Choose Assets/Components for raw-hosted Repository

File *

Choose File

No file selected

Filename *

+ Add another asset

Component attributes

Directory *

Destination for uploaded files (e.g. /path/to/files/)

Tag

Cancel

Upload

Thank You

Contact Us



www.systemex.com

SYSTEMEX 精誠集團