

Couchbase 5.5

사용자 권한 메뉴얼



Secret Management 기능

- 사용자가 디스크에 기밀 정보(Secret으로 칭함)가 암호화된 형식으로 저장되도록 하는 기능
- Secret에는 비밀번호, 인증서 및 Couchbase 내부의 보안 필수 항목이 해당됨.
- 기본적으로 비활성화된 상태이며, 활성화 시 master password를 설정해야 하며 설정을 하고 나면 서버를 시작할 때 입력해야 함
- 비활성화된 상태에서는 빈 암호(키)로 암호화되는데 보안 수준이 떨어진다고 판단되면 Secret Management를 활성화 하는 것을 권장
 - 재부팅이 필요한 작업이니 내부적인 사항을 고려해 결정해야 함
 - 특히 EOL이 지난 서버라면 테스트 서버로 테스트를 충분히 해보는 것을 권장함
- 아래의 그림과 같이 AES 256 알고리즘을 GCM 모드로 사용하여 암호화 계층에서 암호를 암호화함



1. 마스터 암호를 지정하면 Couchbase는 Key Derivation 함수 PBKDF2를 사용하여 Master-key를 파생함
2. 또한 임의의 Data-key를 생성하는데, Master-key로 이 Data-key를 암호화함
3. 이 Data-key는 AES 256 알고리즘을 사용하여 GCM 모드에서 디스크의 모든 secret을 암호화 하는 데에 사용됨

Secret Management 설정

- master password 설정 방법
 - 노드 별로 해당 노드에서 로컬로 실행해야 함
 1. couchbase설치경로/bin 으로 이동
 2. couchbase-cli 를 통해 master-password 설정
\$ couchbase-cli setting-master-password -c 127.0.0.1 -u Administrator기입 -p password기입 --new-password 설정할password기입
 3. 환경 변수 설정
\$ export CB_MASTER_PASSWORD=설정한password기입
 4. Couchbase 서버 재시작 (안되면 2~3번 시도)
 5. 부팅이 완료되면 정상적으로 암호화가 진행됨

사용자 권한 확인

The screenshot shows the N2M Security console interface. The top navigation bar includes 'LDAP', 'ADD GROUP', and 'ADD USER'. The main navigation menu on the left lists 'Dashboard', 'Servers', 'Buckets', 'XDCR', 'Security' (highlighted with a red box), 'Settings', 'Logs', 'Documents', 'Query', 'Indexes', 'Search', 'Analytics', 'Eventing', and 'Views'. The 'Security' section is active, displaying the 'Users & Groups' tab. A search bar 'filter users...' is at the top. Below it, a table lists users. The 'roles' column for the 'n2m_user01' user is highlighted with a red box, showing 'Full Admin'. The 'userAdmin' user has roles 'XDCR Inbound[chatBucket], Application Access[chatBucket], Bucket Admin[chatBucket]'. The table also shows 'auth domain' and 'password set' for each user. At the bottom, there is a pagination control showing '20' and navigation links '< prev | next >'. Status messages at the top right indicate 'sasauthd authentication is not enabled' and 'LDAP is not enabled'.

username	full name	groups	roles	auth domain	password set
n2m_user01	n2m_user01	N2M	Full Admin	Couchbase	22 Apr, 2020
userAdmin	userAdmin		XDCR Inbound[chatBucket], Application Access[chatBucket], Bucket Admin[chatBucket]	Couchbase	23 Aug, 2021

- Web Console의 Security 탭 -> Users & Groups -> roles 부분에서 유저에게 부여한 권한을 확인 가능함
- Security Admin 혹은 Read-Only Admin 권한이 있어야 이 페이지를 확인할 수 있음

사용자 권한 정리 - Global Role

역할	설명	WebConsole Access
Full Admin	보안을 포함한 모든 기능과 리소스에 대한 액세스를 지원함.	O
Cluster Admin	보안을 제외한 모든 클러스터의 기능을 관리할 수 있음. 데이터 액세스는 불가능함.	O
Security Admin	보안 관리자의 역할로, 사용자 역할 관리 및 클러스터의 모든 통계를 확인할 수 있음. 데이터 액세스는 불가능함.	O
Read-Only Admin	클러스터의 통계, 보안 등 읽기만 가능한 권한 데이터 액세스는 불가능함.	O
XDCR Admin	XDCR 기능을 사용해 클러스터 참조 및 복제 스트림을 만들 수 있는 권한	O
Query CURL Access	N1QL CURL 기능을 실행할 수 있도록 허용함.	O
Query System Catalog	System Catalog의 N1QL을 통해 정보를 조회할 수 있도록 허용함. 쿼리를 디버깅해야 하는 트러블슈터를 위해 설계된 역할	O
Analytics Reader	Analytics의 Shadow data-set를 쿼리하는 역할	O

- 다수의 권한을 선택할 수 있음
- ex) Read-Only + Query CURL Access 권한을 부여한 사용자는 Security 탭에서 본인의 권한도 확인할 수 있고 N1QL 실행 권한이 있는 사용자

사용자 권한 정리 - Bucket Role

역할	설명	WebConsole Access
Bucket Admin	Bucket의 모든 기능을 관리할 수 있도록 하는 역할. 데이터의 읽기 및 쓰기는 불가능함.	O
Views Admin	View 데이터에 대한 모든 액세스가 가능함. Bucket 설정 및 데이터를 읽을 수 있음.	O
Search Admin	버킷 별 Search 서비스의 모든 액세스가 가능함.	O
Application Access	데이터 및 N1QL, View, Index 에 대해 액세스가 가능함.	X
Data Reader	데이터를 읽는 것만 가능한 역할. N1QL 실행은 허용하지 않음	X
Data Writer	데이터를 쓰는 것만 가능한 역할.	X
Data DCP Reader	DCP 스트림이 가능하도록 허용하는 역할	X
Data Backup	데이터 백업 및 복원을 가능하게 하는 역할.	X
Data Monitor	통계를 확인할 수 있도록 하는 역할.	X

사용자 권한 정리 - Bucket Role

역할	설명	WebConsole Access
XDCR Inbound	Inbound XDCR 스트림을 생성할 수 있도록 하는 역할	X
Analytics Manager	버킷 별 Analytics 서비스를 관리할 수 있도록 하는 역할	O
Views Reader	View 데이터를 읽을 수 있도록 하는 역할	X
Search Reader	FTS Index를 검색할 수 있도록 하는 역할	O
Query Select	Select Query를 실행할 수 있도록 하는 역할	O
Query Update	Update Query를 실행할 수 있도록 하는 역할	O
Query Insert	Insert Query를 실행할 수 있도록 하는 역할	O
Query Delete	Delete Query를 실행할 수 있도록 하는 역할	O

데이터 확인 테스트

testCluster > Security

LDAPADD GROUPADD USER

Users & GroupsRoot CertificateClient CertificateAuditLog RedactionSession

filter by username...

LDAP is not enabled

UsersGroups

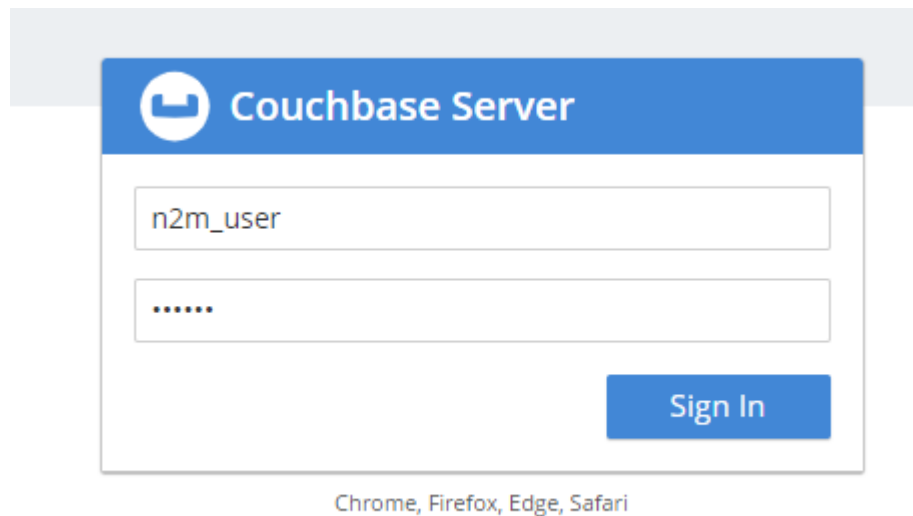
username ▲	groups	roles	auth domain	password set
n2m_user		Query Select [*:*:*] , Data Reader [gamesim-sample:*:*] , Read-Only Admin	Couchbase	24 Aug, 2021
full name: n2m_user				
			Delete	Reset Password
n2m_user2		Read-Only Admin	Couchbase	24 Aug, 2021

20 ▼

< prev | next >

- 테스트용 계정 생성 -> n2m_user
 - 권한 확인을 위한 Read-only Admin 권한
 - gamesim-sample Bucket의 데이터 확인을 위한 Data Reader 권한
 - Query Select 권한 (GUI에서의 Document도 Query Select 권한이 있어야 조회 가능

데이터 확인 테스트



- 해당 유저로 로그인

The screenshot shows the Couchbase Security interface. The top navigation bar includes 'testCluster > Security' and tabs for 'Users & Groups', 'Root Certificate', 'Client Certificate', 'Audit', 'Log Redaction', and 'Session'. The 'Users & Groups' tab is active. On the left, a sidebar menu has 'Security' highlighted with a red box. The main area displays a table of users with columns for 'username', 'groups', 'roles', 'auth domain', and 'password set'. The 'roles' column for the 'n2m_user' entry is highlighted with a red box. A search bar at the top left of the table says 'filter by username...'. A status indicator at the top right says 'LDAP is not enabled'. At the bottom right, there are navigation links '< prev' and 'next >'. A dropdown menu at the bottom left of the table shows the number '20'.

username	groups	roles	auth domain	password set
n2m_user		Query Select [*:~*], Data Reader [gamesim-sample:~*], Read-Only Admin	Couchbase	24 Aug, 2021
n2m_user2		Read-Only Admin	Couchbase	24 Aug, 2021

- Security 탭에서 본인의 권한 확인 가능 < Read-only 이기때문에 수정 불가능 >

데이터 확인 테스트

Dashboard

Servers

Buckets

XDCR

Security

Settings

Logs

Documents

Query

Indexes

Search

Views

Workbench

Import

Keyspace bucket.scope.collection

Limit 10

Offset 0

Document ID optional...

show range









































N1QL WHERE optional...

Retrieve Docs

10 Results for select meta().id from `gamesim-sample`.`_default`.`_default` data order by meta().id limit 10 offset 0

enable field editing

< prev batch | next batch >

	id	
   	Aaron0	{"experience": 14746, "hitpoints": 20210, "jsonType": "pldfdfayer", "level": 146, "loggedIn": true, "name": "Aaron0", "uuid": "3b49dd18-1d56-478e-8ab1-fb38e31ce7e2"}
   	Aaron1	{"experience": 14248, "hitpoints": 23832, "jsonType": "playdfdfasdfsdf", "level": 141, "loggedIn": true, "name": "Aaron1", "uuid": "78edf902-7dd2-49a4-99b4-1c94ee286a33"}
   	Aaron2	{ "experience": 55, "hitpoints": 10, "jsonType": "player", "level": 2, "loggedIn": true, "name": "Aaron2", "uuid": "edc5aedef-9cb6-4c11-90d4-9645083053e8" }
   	Aliaksey0	{ "experience": 327, "hitpoints": 10, "jsonType": "player", "level": 2, "loggedIn": true, "name": "Aliaksey0", "uuid": "788cb5c6-905f-4509-ae1b-9dd66f4b72a8" }
   	Aliaksey1	{ "experience": 17263, "hitpoints": 25622, "jsonType": "player", "level": 172, "loggedIn": true, "name": "Aliaksey1", "uuid": "470f297b-31a4-4571-a8a9-6baa80c87355" }...
   	Aliaksey2	{ "experience": 326, "hitpoints": 10, "jsonType": "player", "level": 2, "loggedIn": true, "name": "Aliaksey2", "uuid": "d4c898a1-104b-436a-8bd7-6711046d2c23" }
   	Axe_14e3ad7b-8469-444e-8057-ac5aefcdf89e	{ "jsonType": "item", "name": "Axe_14e3ad7b-8469-444e-8057-ac5aefcdf89e", "uuid": "14e3ad7b-8469-444e-8057-ac5aefcdf89e", "ownerId": "Benjamin2" }
   	Axe_153cc5ac-f542-4f29-a20a-6333112ae338	{ "jsonType": "item", "name": "Axe_153cc5ac-f542-4f29-a20a-6333112ae338", "uuid": "153cc5ac-f542-4f29-a20a-6333112ae338", "ownerId": "Srini2" }
   	Axe_17ef27b7-ce41-4488-953e-bd9d380a002c	{ "jsonType": "item", "name": "Axe_17ef27b7-ce41-4488-953e-bd9d380a002c", "uuid": "17ef27b7-ce41-4488-953e-bd9d380a002c", "ownerId": "Leila0" }
   	Axe_1a728223-af6e-4666-af50-199d99d2c7d1	{ "jsonType": "item", "name": "Axe_1a728223-af6e-4666-af50-199d99d2c7d1", "uuid": "1a728223-af6e-4666-af50-199d99d2c7d1", "ownerId": "Volker1" }

- Document 탭에서 데이터 조회 가능.
- 수정 시 Forbidden 에러 발생 < 수정 권한을 부여받지 못한 계정이기때문에 >