

# CREATE IBM CLOUDANT

TEAM ID : PNT2022TMID48397

PROJECT : SMART WASTE MANAGEMENT SYSTEM FOR METROPOLITAN CITIES

The screenshot shows the IBM Cloud console interface. The top navigation bar includes the IBM Cloud logo, a search bar, and user information. The main content area displays the 'Overview' tab for a specific Cloudant instance. The instance name is 'node-red-wtkms-2022--cloudant-1667206654531', and its status is 'Active'. The left sidebar contains a 'Manage' section with links to 'Service credentials', 'Plan', and 'Connections'. The main content area includes a 'Launch Dashboard' button and a 'Deployment details' section with the following information:

- CRN:** crm:v1:bluemixpublic:cloudantnosqldb:au-syd:a/2661d24370904cfc91397dc2362fe6f2:1d60a430-11b4-47d7-afc7-a375af6d8938::
- Location:** Sydney
- External endpoint:** <https://9a890b08-352e-4539-afaf-33cb36d34cf9-bluemix.cloudant.com>
- External endpoint (preferred):** <https://9a890b08-352e-4539-afaf-33cb36d34cf9-bluemix.cloudantnosqldb.appdomain.cloud>
- Authentication methods:** IBM Cloud IAM and Cloudant credentials. A 'Migrate to IAM Only' button is present.
- Activity Tracker event types:** A dropdown menu is set to 'Management'.
- Disk encryption:** Yes. Automatically generated disk encryption key.

The screenshot shows the same IBM Cloud console interface, but with the 'Docs' tab selected. The main content area displays documentation for the Cloudant instance. The documentation includes a warning about TLS 1.0 and 1.1, a section on 'IBM Identity & Access Management (IAM)', and a section on 'IBM Cloudant Dedicated Hardware environment security enhancements'.

**Warning:** Starting on September 2022, the IBM Cloudant service will require Transport Layer Security (TLS) 1.2 and above. The IBM Cloudant service requires TLS 1.2 and currently supports TLS 1.2 and above. If your applications are still using TLS 1.0 or 1.1, please update them immediately to TLS 1.2 or above to avoid any impact. If you are unsure what TLS version your application is using to connect to Cloudant or have any questions, open a support ticket. See IBM Cloudant security docs for more detail.

**IBM Identity & Access Management (IAM)**  
IBM Cloudant instances in the IBM Cloud now support IBM IAM for authentication and authorization. IBM IAM allows for centralized control for granting user and programmatic access to all the Cloudant instances in your IBM Cloud account. See the [IAM guide](#) in the documentation for a comparison between using IAM and legacy Cloudant authentication for your applications. In addition, IBM Cloudant instances support Resource Groups and we encourage all customers to migrate their Cloudant instances that remain in a Cloud Foundry space to Resource Groups to take advantage of the security access benefits. See the [FAQ](#) on using Cloudant with Resource Groups for more details.

**IBM Cloudant Dedicated Hardware environment security enhancements**  
The IBM Cloudant Dedicated Hardware plan in the IBM Cloud catalog is for customers who require additional security and compliance benefits. IBM Cloudant Dedicated Hardware instances are isolated environments for the sole use of a customer to run one or more IBM Cloudant Standard plan instances. We have added the ability to connect via IBM's internal network, meaning customers can avoid public network and outbound bandwidth costs when connecting to Cloudant from their applications. With that, Dedicated Hardware environment now offer the following benefits:

- Isolation at the database compute and storage layers for a single customer
- Choice of any [IBM Cloud location](#)
- Optional HIPAA readiness in US locations
- Both external and internal [service endpoints](#)
- IP whitelisting
- Bring your own encryption key (BYOK) with Key Protect