NC-CCDC Team Document

An Overview of Systems, Environment and Scenario

Table Of Contents

Table Of Contents 1

Scenario Information 3

System Documentation 4

- List of Systems 4
- Systems In Depth 5
  - Firewall 5
  - DC01 5
  - DC02 5
  - DHCP01 6
  - DOCK01 6
  - DB01 6
  - DB02 6
  - WEB01 6
  - WEB02 7
  - WEB03 7
  - WEB04 7
  - FS01 7
  - CA01 8
  - REPO01 8
  - ROOTCA01 8

Mt. CCDC Web-App Documentation 9

- Basic Architecture 9
- Configuration and Setup 9
  - WEB01 Setup 9
    - Config Descriptions 10
      - dbHost 10
      - dbDatabase 10
      - dbUser 10
      - dbPassword 10
      - webAppSessionSecretKey 10
      - logFile 10
      - logMaxBytes 10
      - logBackups 10

ldapHost 10
ldapUser 10
ldapPassword 11
ldapBaseDN 11
domain 11
adminGroup 11
webUsersGroup 11
Wallet RPC 11
RPC User 11
RPC Password 11
RPC Address 11
RPC Port 11
Transaction Interval 11
Logging 11
CA01 Setup 11
DB01 Setup 12

Communication Documentation **12**
Configuration and Setup 12

Scenario Information

From: Office of the CEO <thebigboss@mtccdc.com>

Subject: Welcome to the Team!

To: "Operations Team" <teamx@youllfindthisoutlater.com>

Hey! Welcome to the team!

I'm the CEO of Mt. CCDC. I am proud to lead one of the most hip and progressive companies since the dawn of BookFace! We have so much fun around here!

In these uncertain financial times, cash and stocks are so 2010. We're moving forward baby! This is 2019, where COIN is life! I really don't know much about it myself, but I know it's the future and if we don't start now we'll be left behind! There's all these buzzwords - blockchain, wallets, coins, mining. It reminds me of panning for gold, but techy! Enter: DakotaCoin. With its recent rise in popularity and no real exchanges to trade it yet we saw a market opportunity to fill that void! We are now among the top 10 DakotaCoin exchanges in the world today!

So. Anyway. Welcome to the team! We've gotten pretty big so I knew our IT guy, Joe Saunders, needed a hand. He's pretty chill, you'll like him. Also, you'll have to get acquainted with James R. Hackler - he's our lead developer here at Mt. CCDC and I like to think of him as a rockstar! He's earned every "penny" of his ridiculously large DakotaCoin salary.

Oh yea, I almost forgot! Speaking of salary - your sizeable salary, benefits, and 401k plans are all backed by DakotaCoin! Isn't that great?! If the company does really well, we might even give out DakotaCoin bonuses this year! DO YOUR BEST!

If you need any clarifications, please put together a list and I'll send it along to Joe and James and tell them to answer what they can!

Sincerely,

Elliott B.
CEO (aka - The Big Boss)

System Documentation

List of Systems

- **Firewall**
  - OS: PanOS 8.0
  - MGMT IP: 192.168.1.2
  - Gateway IP:192.168.1.1
- **DC01**
  - Purpose: Primary DC
    - Domain: ccdc.local
  - OS: Windows 2016
  - IP: 192.168.1.10
- **DC02**
  - Purpose: Secondary DC
  - OS: Windows 2019
  - IP: 192.168.1.15
- **DHCP01**
  - Purpose: DHCP Server
  - OS: FreeBSD 10.3
  - IP: 192.168.1.20
  - DHCP range 192.168.1.100 - 192.168.1.249
- **DOCK01**
  - Purpose: Docker Host
  - OS: Ubuntu 16.04 LTS
  - IP: 192.168.1.24
- **DB01**
  - Purpose: MS-SQL Crypto Exchange web app backend
  - OS: Ubuntu 16.04 LTS
  - IP: 192.168.1.25
- **DB02**
  - Purpose: MariaDB for assorted web-apps and HR
  - OS: Ubuntu 16.04 LTS
  - IP: 192.168.1.30
- **WEB01**
  - Purpose: Mt. CCDC web-app host
  - OS: Ubuntu 16.04.2 LTS
  - IP: 192.168.1.50
- **WEB02**
  - Purpose: IIS+PHP, Employee Onboarding website
  - OS: Windows 2012
  - IP: 192.168.1.55
- **WEB03**
  - Purpose: Apache2+PHP, Internal services (wiki, etc)
  - OS: Ubuntu 16.04
  - IP: 192.168.1.60

- **WEB04**
  - Purpose: Container Control for DOCK01
  - OS: Ubuntu 16.04 LTS
  - IP: 192.168.1.65
- **FS01**
  - Purpose: SMB/FTP file share
  - OS: Windows 2008 R2
  - IP: 192.168.1.70
- **CA01**
  - Purpose: Mt. CCDC wallet RPC
  - OS: Ubuntu 18.04.2 LTS
  - IP: 192.168.1.75
- **REPO01**
  - Purpose: git code repo
  - OS: Ubuntu 16.04
  - IP: 192.168.1.80
- **ROOTCA01**
  - Purpose: Root CA for the domain
  - OS: Windows Server 2016
  - IP: 192.168.1.95

Systems In Depth

Firewall

This is our next gen firewall that the sales guy said would make our network super secure and not have to worry about hackers anymore. Does 1:1 nat translation from our private IP space to our public IP's. Also acts as our switch for the IT department.

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

DC01

Primary DC for the Mt. CCDC Windows Domain, also provides DNS

Dependencies:

- DC02 - For replication
- ROOTCA01 - For LDAPS

Scored Services:

- LDAP
- DNS

DC02

Backup DC for the Mt. CCDC Windows Domain, also provides backup DNS

Dependencies:

- DC01 - For replication
- ROOTCA01 - For LDAPS

Scored Services:

- LDAP
- DNS

DHCP01

Provides DHCP for end user client devices

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- SSH

DOCK01

Server James asked me to spin up so he could try "containerizing our services". IMO they should still be separate hosts to prevent a single point of failure but no one listens to ol' Joe do they! TBH I'm not sure what all is running on it but James did say something about moving some of his web-app's dependencies onto it.

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- SSH

DB01

Database server for the Mt. CCDC DakotaCoin exchange web-app on WEB01. Hosts a MSSQL database containing user information, and transaction history for all transactions originating from Mt. CCDC. It also holds some configuration information for how the web-app should access the wallet RPC located at CA01.

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- MSSQL

DB02

MySQL database which hosts databases for HR to store employee data and the onboarding Wordpress app. Also supports our internal wiki.

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- MySQL

WEB01

Primary host for the web server and business logic for Mt. CCDC. Running an Apache2 web server with `mod_wsgi` to interface with the business logic.

More detailed information on how to run and manage the web-app can be found in the section Mt. CCDC Web-App Documentation.

Dependencies:

- DB01 - Database access for transaction, user and some config management.

- DC01 - User authentication and DNS
- CA01 - To access the DakotaCoin network and handle off platform transactions
- DC02 - Backup DNS

Scored Services:

- HTTP

WEB02

Employee Onboarding server. All employees must be able to log into this site. New employees accounts must be created and tested.

Dependencies:

- DC01 - LDAP, DNS
- DC02 - Backup LDAP, Backup DNS

Scored Services:

- HTTP

WEB03

Internal company wiki. We haven't been very good about keeping it up to date, but this is where we will put all of our employee guides and system information once we get around to it!

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS
- DB02 - Backing database

Scored Services:

- HTTP
- SSH

WEB04

According to James, this is supposed to help him control what docker containers are running on DOCK01.

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- HTTP

FS01

Joe gave me this server to use as a File Share and it hosts important files for the company. Files must be accessible via both SMB and FTP. He did say something about it being a DC before I turned it into the File Share

Dependencies:

- DC01 - LDAP, DNS
- DC02 - Backup LDAP, Backup DNS

Scored Services:

- FTP
- SMB

CA01

This hosts our DakotaCoin wallet and associated RPC for programmatic access. Satoshi Nakamoto created a great little JSON RPC for managing wallets, accounts, and address and as DakotaCoin is a fork from Litecoin 0.8.5.1, it sure made our life easier when we were building this exchange. That said his documentation kinda sucks. If the need to execute RPC calls manually were to arise, In `dakotacoin-qt` there is a `Help` drop down menu from which you can access a `Debug Window` which allows for manual RPC calls. Just be careful to double check addresses!

Dependencies:

- 10.0.0.20 - DakotaCoin bootstrap node
- 10.0.0.21 - DakotaCoin bootstrap node
- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- Wallet Service

REPO01

This is our Git repository for all our code. It currently indexes our wiki and our crypto exchange platform. If anything were to go wrong with those sites at least we have backups here!

Dependencies:

- DC01 - DNS
- DC02 - Backup DNS

Scored Services:

- HTTP
- SSH

ROOTCA01

Acts as a certificate authority for the domain allowing us to do LDAPS.

Dependencies:

- DC01 - DNS and AD
- DC02 - Backup DNS and AD

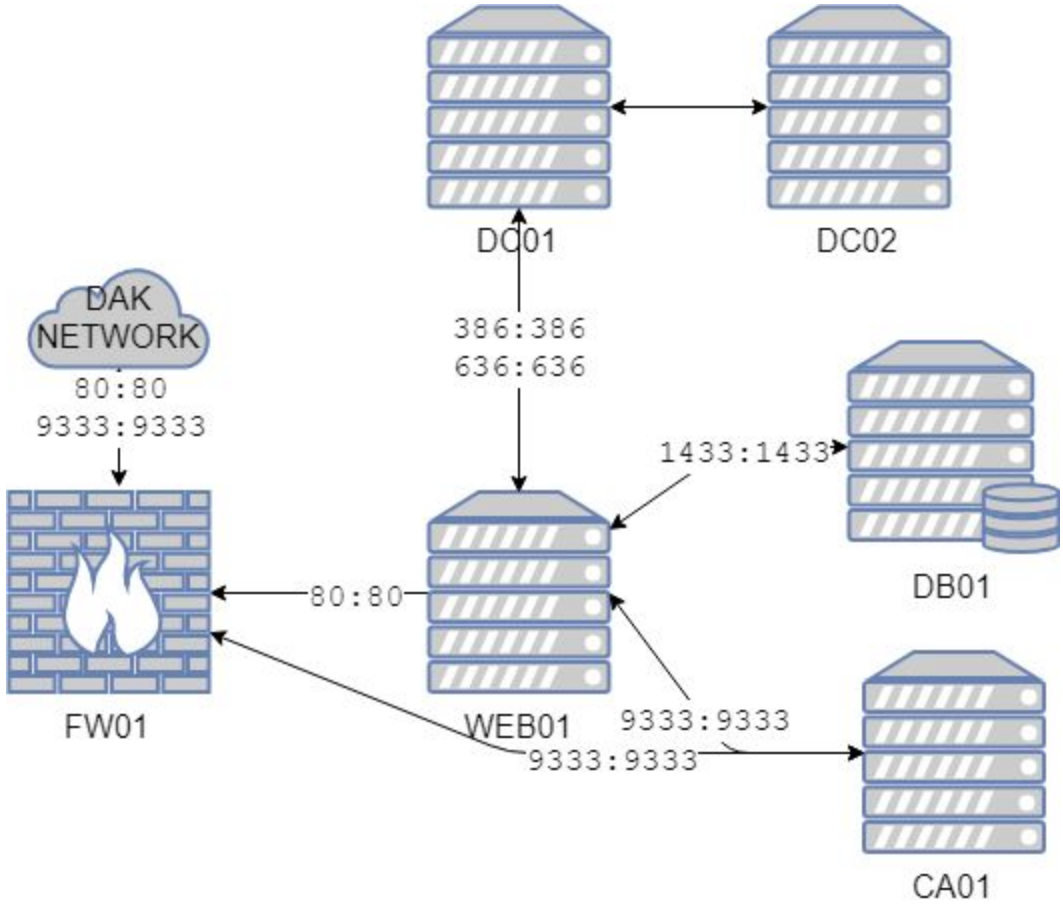
Scored Services:

- (none)

Mt. CCDC Web-App Documentation

This section will give a brief description of how to set up, run, and use the DakotaCoin exchange here at Mt. CCDC. Hopefully, after reading this document you should have a working understanding of how to keep things working. Unlike Joe Joe.

Basic Architecture



The figure above shows the overall dependency graph of services required to run the exchange. The core of the exchange is WEB01 that is where the Apache2 web server for the exchange and the business logic live. It is dependent on DB01 for tracking user information, transaction history, and certain configuration information. It also depends of DC01 for user authentication using LDAPS. The choice to use LDAPS to handle user auth was made in an effort to improve our security posture by offloading the technical effort to correctly handle passwords to a third party. This should reduce or eliminate any chance of a malicious actor accessing users accounts (and their associated funds). via our mishandling of passwords. CA01 is where our wallet lives, as such it requires access to the internet so it can communicate with the rest of the DakotaCoin network to perform transactions.

Configuration and Setup

WEB01 Setup

WEB01, is the primary web server and business logic processing host for Mt. CCDC. The

exchange runs off of an Apache2 web server using Python 3.5.2 under `mod_wsgi` and the Flask framework. The configuration file for the apache site can be found at: `/etc/apache2/sites-enabled/000-default.conf`. The primary configuration file for the DAK exchange can be found at `/var/www/NCCDC-DakotaCoin/exchange/config.json`. This file is essentially the same as the one shown in the image below, except for the fact that the values are populated with actual values. Some of which are listed below as well.

Config Descriptions

- **dbHost**
  - The hostname or IP address of the MSSQL server on which the database is hosted. Currently this is `DB01.ccdc.local`.
- **dbDatabase**
  - The name of the database on the MSSQL server which is to be used. Currently this is the `exchange` database
- **dbUser**
  - The user the application will use to login to the database. Currently we are using the `sa` user.
- **dbPassword**
  - The password for the database user specified in `dbUser`. Currently this is `Password1!`.
- **webAppSessionSecretKey**
  - The secret key for signing session cookie data with.
- **logFile**
  - The path to the log file which will store user access times, IP address and some session info, additionally if a request causes internal server errors those will be stored as well in the form of a Python stack trace. Currently this is set to `exchange.log`.
- **logMaxBytes**
  - The maximum size the log file will reach. Currently this is set to `100000` bytes.
- **logBackups**
  - How many backups should be kept of the log file if it reaches the size of `logMaxBytes`. Currently this is set to `1`. (So if the log fills, a new one will be created and once the new log file fills the backup will be replaced with the newly full one and another new empty log file will be created. Exact details of what I'm trying to explain can be found here).
- **ldapHost**
  - The hostname or IP address of LDAP server we will auth users against. Currently this is set to `DC01.ccdc.local`.
- **ldapUser**
  - The user used for account management. Currently this is set to `ccdc\Administrator`.

- **ldapPassword**
  - The password of the account specified in ldapUser. Currently this is set to `Password1!`.
- **ldapBaseDN**
  - The base distinguished name from which user will be created. Currently this is set to `CN=Users,DC=ccdc,DC=local`.
- **domain**
  - The name of the AD domain this setting is used in the creation of, and authentication of users. Currently this is `ccdc.local`.
- **adminGroup**
  - The OU/Group web app administrators belong to. Currently this is set to `Web App Admins`.
- **webUsersGroup**
  - The DN of the OU/Group we app users belong to and are added to upon creation. Currently this is set to `CN=Web App Users,CN=Users,DC=ccdc,DC=local`.

To set configuration regarding access to the wallet RPC, login as as a user in the group and navigate to `/admin`. From there you can set the host, username, password and port of the wallet RPC. You can also set the interval at which transactions are made.

Wallet RPC

- **RPC User**
  - The username set in the `dakotacoin.conf`. Currently this is set to `username`.
- **RPC Password**
  - The username set in the `dakotacoin.conf`. Currently this is set to `Password1!`.
- **RPC Address**
  - The hostname or IP address of the wallet RPC host. Currently this is set to `CA01.ccdc.local`.
- **RPC Port**
  - The port on which to connect to the RPC. Currently this is set to `9332`.
- **Transaction Interval**
  - The interval between when batches of transactions are sent off the the RPC currently this is set to `60` seconds.

Logging

Logging for errors related directly to the Python application is currently set up to be under `/home/webadmin/exchange.log`. Logging related to Apache2 or mod_wsgi is under `/var/log/apache2/`.

CA01 Setup

Setting up CA01 is a fairly simple matter after getting the DakotaCoin wallet compiled. All one needs do is create a `dakotacoin.conf` file in the current user's home directory in a

directory called `.dakotacoin`. So the path would boil down to: `~/.dakotacoin/dakotacoin.conf` Simply run the executable `dakotacoin-qt`, which is currently located in `/home/walletadmin/NCCDC-DakotaCoin/dakotacoin`. Currently this config file exists, however if it ever were to be deleted it is critical to include the following lines:

```
addnode=10.0.0.20
addnode=10.0.0.21
```

These lines ensure that the wallet can find the rest of the DakotaCoin network via the bootstrap nodes at `10.0.0.20` and `10.0.0.21`. These lines must be included along with lines to set the user, password, port and IPs in a similar fashion to the photo.

When the system is rebooted be sure to start the DakotaCoin wallet, as it does not start automatically.

DB01 Setup

Setup of DB01 is fairly simple after installing MSSQL Server get a copy of the `dbInit.sql` script from REPO01 and run it against the server. It should create all databases, tables and views required. The script should be located in `NCCDC-DakotaCoin/exchange`. To interact with the database use `/opt/mssql-tools/bin/sqlcmd -S localhost -U sa -P <password>`

Communication Documentation

This section will give a brief description of the internal communications at Mt. CCDC. Here at Mt. CCDC we are a progressive company. As such, all of our communications, documents, and interactions exist in Office 365.

Configuration and Setup

The team has a preconfigured Sharepoint site, Teams site, Exchange inbox, etc. You can use these services as you see fit. You can install the thick clients on computers if you'd like or use the web services only. A forewarning: ALL communications are fully audited and (for security, and theft prevention) outside communications are blocked.

Teams: Used for instant messaging and inject handling. Your team consists of you, the CEO, White Team, and James Hackler.

Sharepoint: Used for inject handling and file storage. Members consist of you, the CEO, White Team, and James Hackler.

Exchange: Used for email, inject handling, etc.