Linde Group

Technology • Strategy • Integrity

JAMF software

JAMF NATION user conference

Linde Group

Technology ▪ Strategy ▪ Integrity

JAMF software

Ghost in the Cloud

Deploying the JSS on Amazon Elastic Compute Cloud (EC2)

JAMF NATION user conference

Linde Group

Technology ▪ Strategy ▪ Integrity

JAMF software

James Barclay

Senior IT Consultant

The Linde Group, Inc.

JAMF NATION user conference

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Deploying the JSS on Amazon EC2

Presentation agenda:

The five Ws (who, what, where, when, and why)

Initial goals and current solution

Making it work

What's it like? (production experiences)

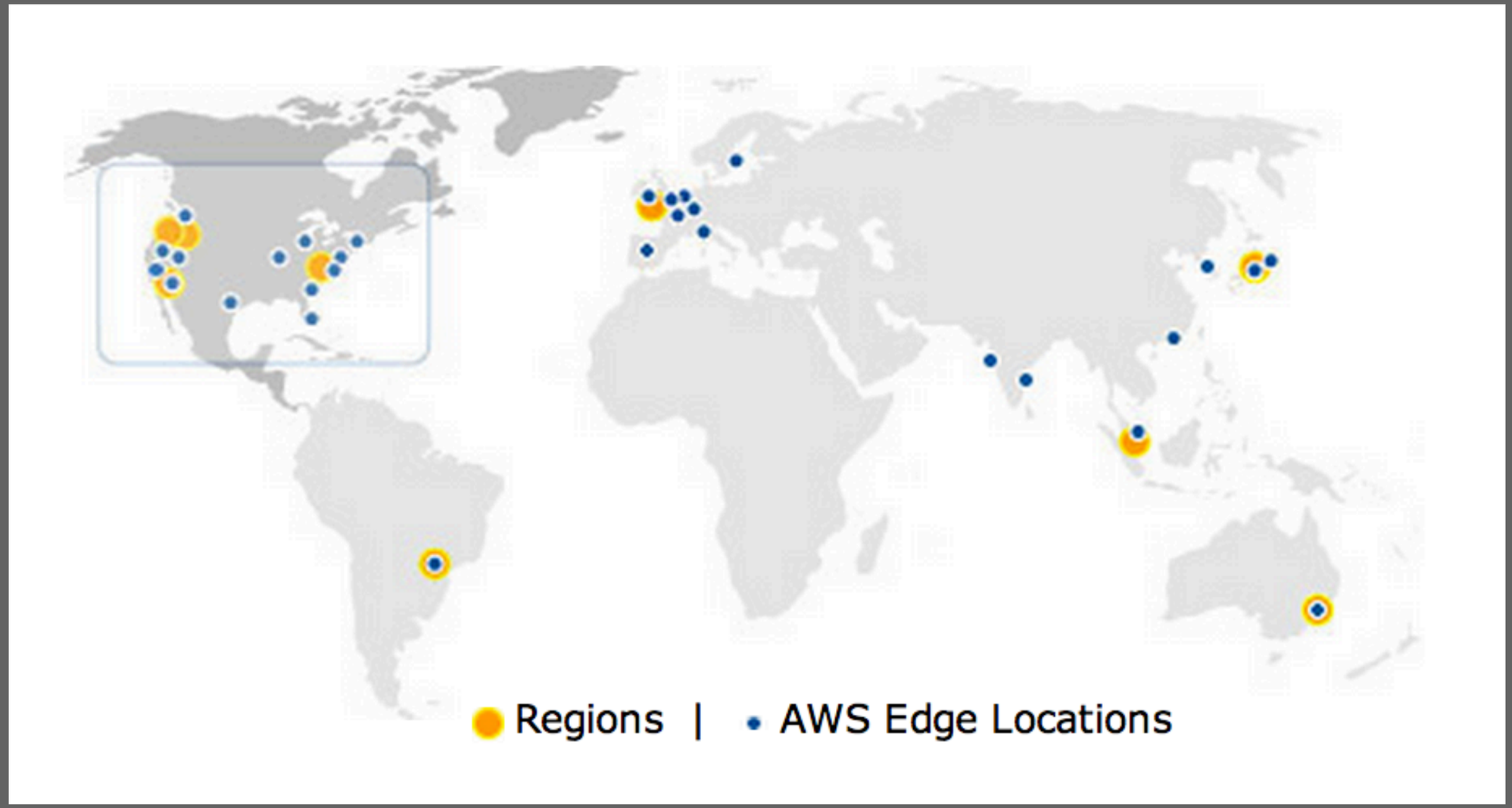
Challenges and limitations

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

The Five Ws of Hosting on EC2

- What is EC2, anyway?
  - A web service that provides **resizable** compute capacity in the cloud
- Who should do this?
  - Startups, companies making use of AWS internally, etc.
- Where is this cloud?
  - Geographically distributed
- When should I do this?
  - When your organization tires of hosting infrastructure themselves
- Why would I do this?
  - Your organization is already using AWS for everything, and they'd prefer to keep it that way
  - You have multiple sites that are geographically distributed



Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Initial Goals

- Start small (.large)
  - Single M1.large Ubuntu instance for JSS, Distribution Point, and MySQL database
- Make it secure
  - Force HTTPS communication, HTTPS authenticated downloads, alternate SSH port, public Tomcat certificate, accessible only behind firewall (office, VPN)
- Document everything
  - So it's easy to reproduce if we ever need to tear it down

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Current Solution

- One M1.large Ubuntu Instance for the JSS
- Two distribution points
  - One using EC2 instance store, one running on an on-site Mac mini
- One M1.large Instance for MySQL database
  - ...with nightly snapshots to Amazon S3 (Simple Storage Service)

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Making it work

- Sign up for a free Amazon Web Services account
  - aws.amazon.com
- Provision a Linux (or Windows Server) EC2 instance
  - JSS Requirements
    - A 64-bit capable Intel processor
    - 2 GB of RAM
    - 400 MB of disk space available

- M1.medium Instance Details
  - A 64-bit capable Intel processor, (1 vCPU, Intel Xeon family)
  - 3.75 GiB of RAM
  - 410 GB of instance store disk space available
- M1.medium Instance Details
  - A 64-bit capable Intel processor (2 vCPU, Intel Xeon family)
  - 7.5 GiB of RAM
  - 420 GB of instance store disk space available

Instance Family	Instance Type	Processor Arch	vCPU	ECU	Physical Processor	Intel® AES-NI	Intel® AVX	Intel® Turbo
General purpose	m1.small	32-bit or 64-bit	1	1	Intel Xeon Family	-	-	-
General purpose	m1.medium	32-bit or 64-bit	1	2	Intel Xeon Family	-	-	-
General purpose	m1.large	64-bit	2	4	Intel Xeon Family	-	-	-
General purpose	m1.xlarge	64-bit	4	8	Intel Xeon Family	-	-	-
General purpose	m3.xlarge	64-bit	4	13	Intel Xeon E5-2670	Yes	-	-
General purpose	m3.2xlarge	64-bit	8	26	Intel Xeon E5-2670	Yes	-	-

- Create a new key pair
  - Choose a descriptive name, (e.g., jss)
  - Download the private key (Keep this safe)
- Configure a security group
  - A security group acts as a firewall that controls the traffic for one or more instances
  - 80, 443, 22, 8443, 8080, 445
- Create and attach an EBS volume to instance
  - Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances
- Launch your instance

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

- Get public IP from EC2 Management Console
- Configure DNS, (Route 53)
- SSH into the instance
  - Copy your private key to ~/.ssh/
  - Create (or append) SSH config file
  - Type `ssh jss` to connect to your instance

JAMF NATION user conference

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Configure the instance

- `sudo apt-get update`
- `sudo apt-get install openjdk-6-jdk`
- `sudo apt-get install mysql-server`
- `mysql -u root -p` (enter password when prompted)
  - `CREATE DATABASE jamfsoftware;`
  - `GRANT ALL ON jamfsoftware.* TO 'jamfsoftware'@localhost IDENTIFIED BY 'passwordbutnotthisone';`

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Install the JSS

- Download the JSS Installer and copy to the instance
  - `scp /path/to/JSSInstallerLinux8.72.zip jss:/home/<user_name>/`
- Unzip the archive
  - `unzip JSSInstallerLinux8.72.zip`
- Run the JSS Installer
  - `sudo /home/<user_name>/jssinstaller.run`

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Configure the JSS

- Point browser to https://jss001.ec2.example.com:8443/
- Complete the initial JSS Setup

JAMF NATION user conference

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

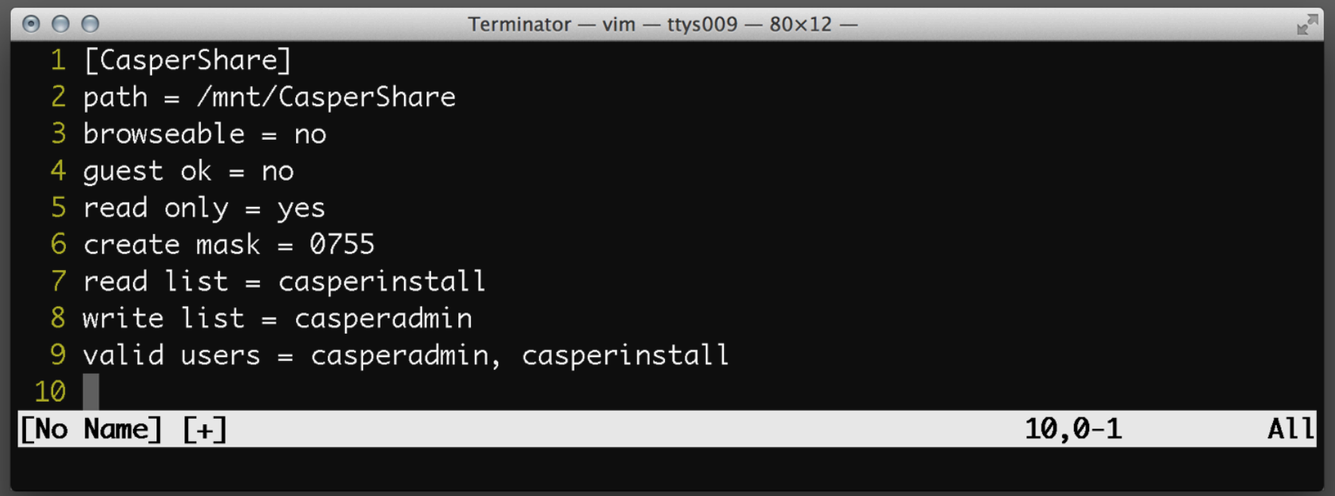
Configure Samba

for use with Casper Admin

- `mkdir /mnt/CasperShare`
- `sudo apt-get install samba; Y`
- `sudo useradd -d /dev/null -s /dev/false casperadmin`
- `sudo useradd -d /dev/null -s /dev/false casperinstall`
- `sudo smbpasswd -a casperadmin`
- `sudo smbpasswd -a casperinstall`

Configure Samba, cont.

- `sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak`
- `sudo vi /etc/samba/smb.conf`



Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Configure Samba, cont.

- `sudo chown casperadmin /mnt/CasperShare`
- `sudo service smbd restart`
- Test connectivity to smb://jss001.ec2.example.com/CasperShare/
- Specify allowed inbound IPs in EC2 Security Groups so Samba is not open to everyone

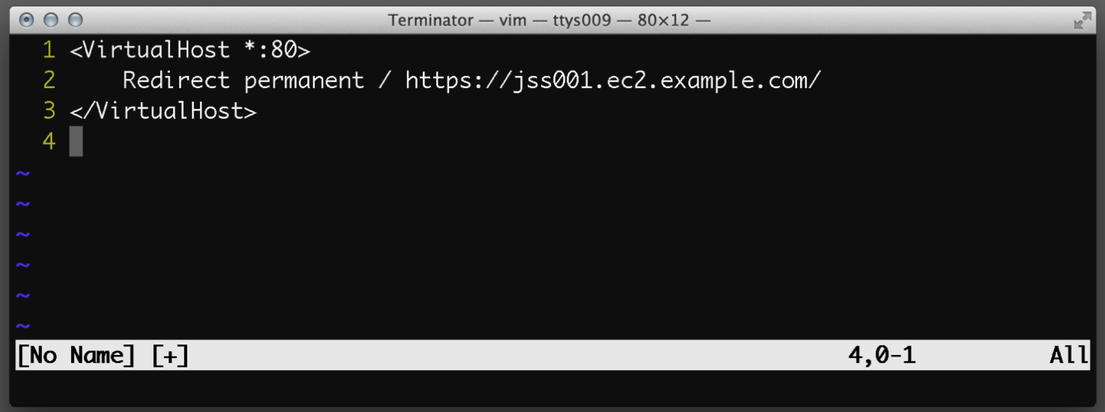
Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Install and configure Apache

for HTTPS downloads

- `sudo apt-get install apache2`
- `sudo apt-get install apache2.2-common`
- `sudo vi /etc/apache2/sites-available/CasperShare`



JAMF NATION user conference

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Install and configure Apache, cont.

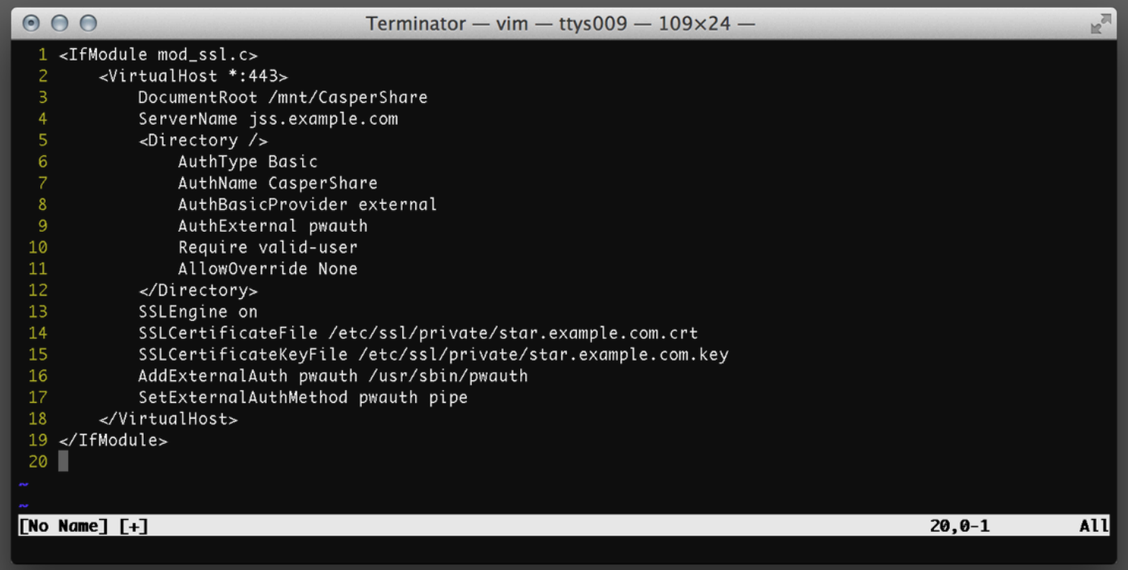
- Obtain a trusted SSL certificate
- Copy certificate to `/etc/ssl/private/`
- `sudo a2enmod ssl`
- `sudo apt-get install libapache2-mod-authnz-external`
- `sudo a2enmod authnz_external`
- `sudo passwd casperinstall`
  - Create a password when prompted

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Install and configure Apache, cont.

- `sudo vi /etc/apache2/sites-available/CasperShare-ssl`



JAMF NATION user conference

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Install and configure Apache, cont.

- `sudo a2dissite default`
- `sudo a2ensite CasperShare`
- `sudo a2ensite CasperShare-ssl`
- Add Alias directive to `/etc/apache2/httpd.conf`
  - `Alias /CasperShare "/mnt/CasperShare"`
- `sudo service apache2 restart`

Testing HTTPS Downloads

- Test HTTPS downloads in a browser by going to https://jss.example.com/CasperShare
- Test HTTPS downloads with cURL
  - `curl -vv -u casperinstall:supersecretpassword https://jss.example.com/CasperShare/Packages/test.dmg` > ~/Desktop/test.dmg

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Enabling SSL on Tomcat

...with a public certificate

- This can vary depending on distribution or CA
  - `sudo su`
  - `cd /usr/local/jss/tomcat`
  - `openssl pkcs12 -export -in /etc/ssl/private/star.example.com.crt -inkey /etc/ssl/private/star.example.com.key -out star.example.com.p12 -name star_example -CAfile bundle.crt -caname root`
    - Enter export password when prompted

Linde Group
Technology ▪ Strategy ▪ Integrity

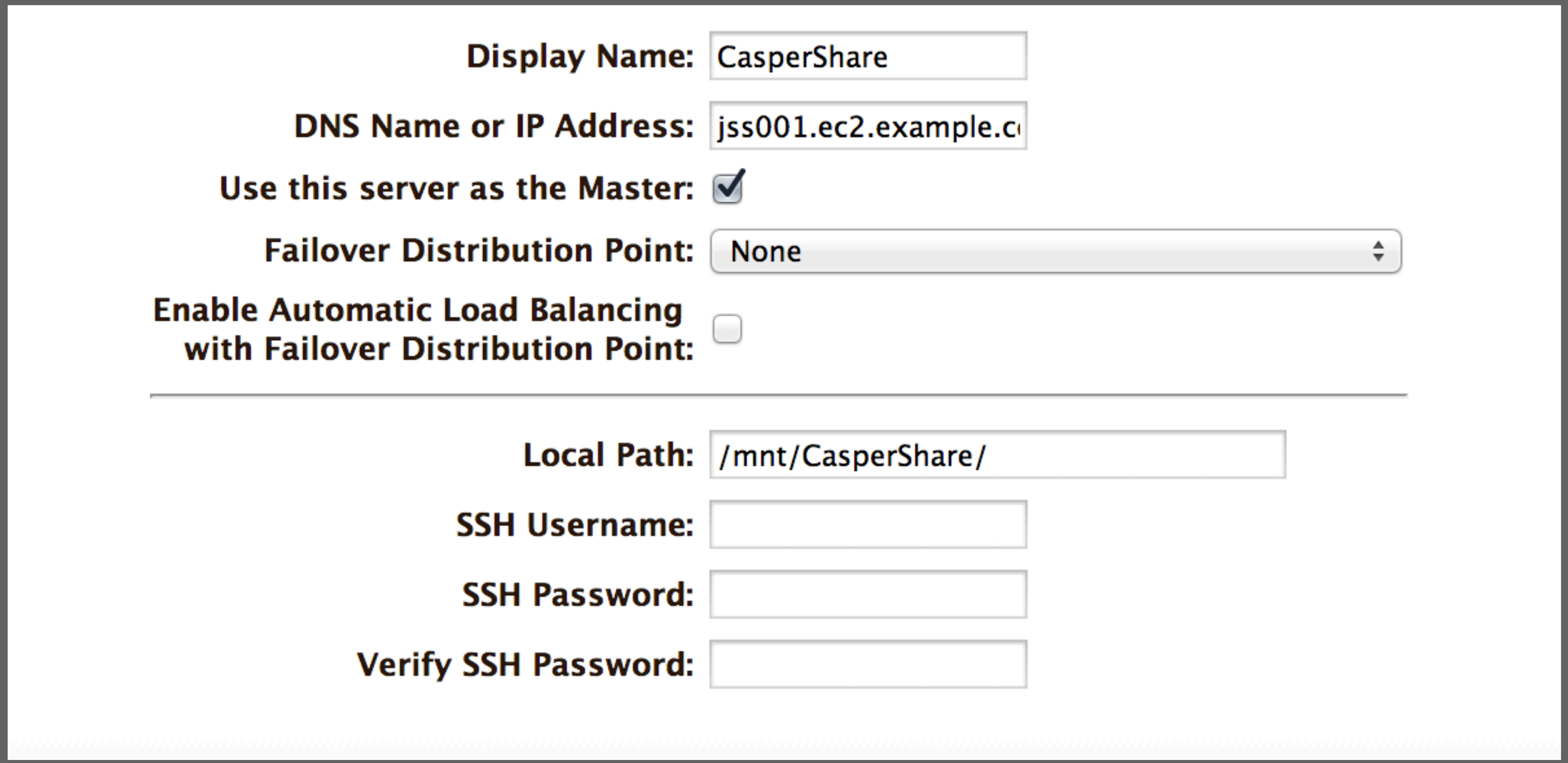
JAMF software

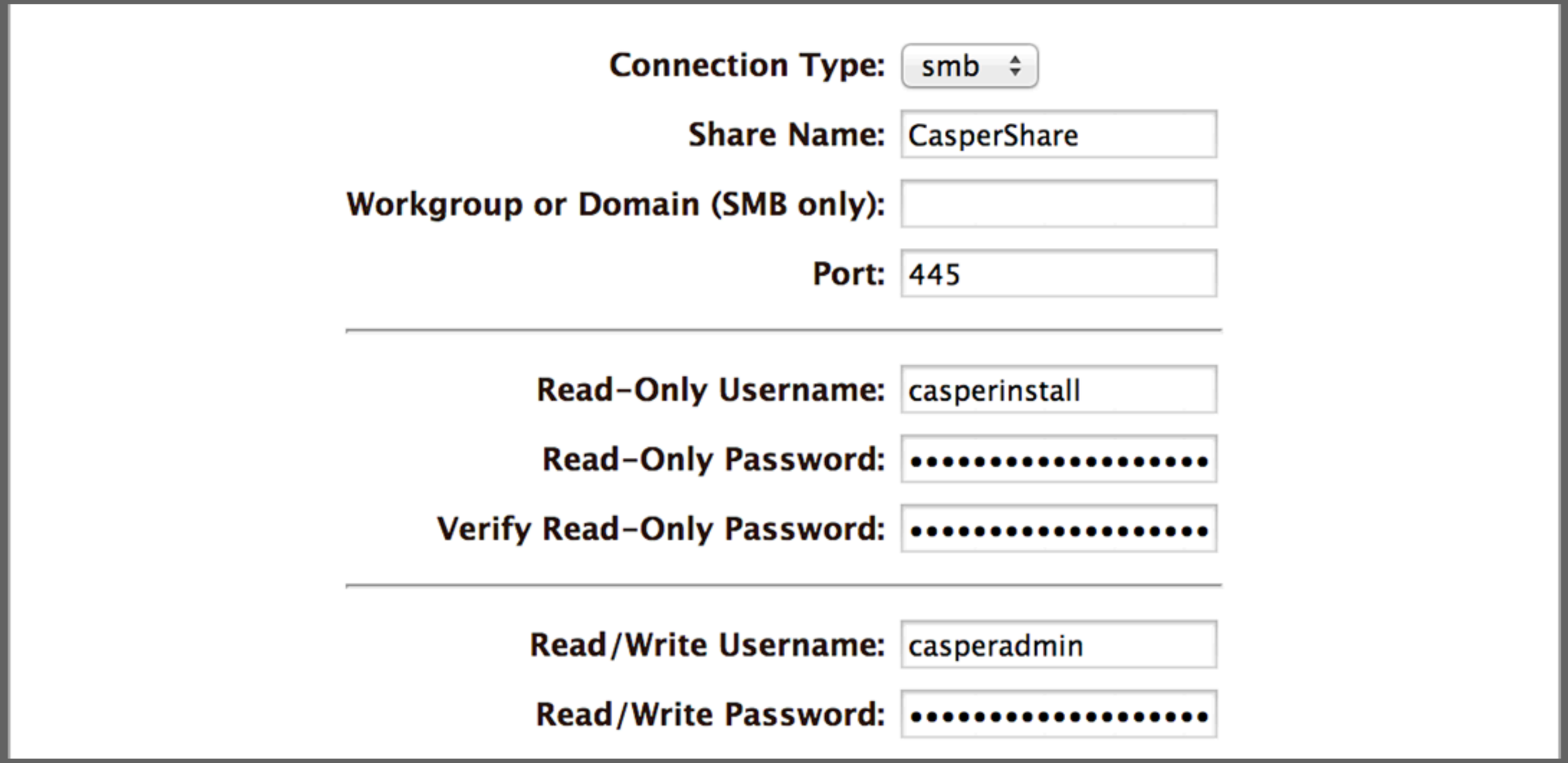
Enabling SSL on Tomcat, cont.

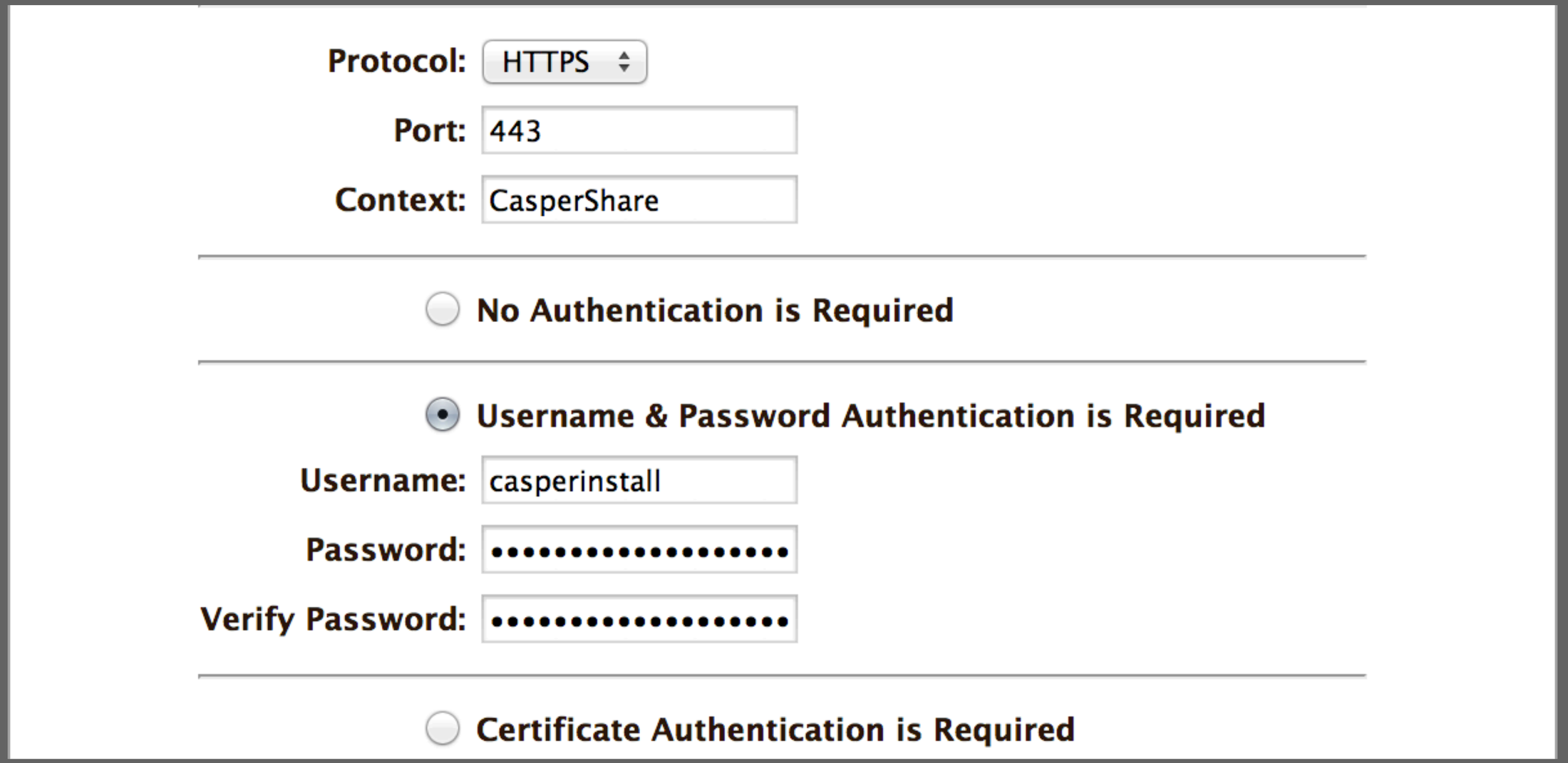
- `keytool -importkeystore -deststorepass supersecretpassword -destkeystore keystore.jks -srckeystore star.example.com.p12 -srcstoretype PKCS12 -srcstorepass supersecretpassword -alias star_example`
- `mv keystore.jks /usr/local/jss/tomcat/.keystore`
- `sudo /etc/init.d/jamf.tomcat7 restart`
- Confirm that the JSS is using your public certificate by testing in a browser

Configuring Distribution Points

- Log in to the JSS at https://jss001.ec2.example.com:8443/
  - Configure your EC2 distribution point by going to *Settings* > *Servers* > *Distribution Points* > *Add Distribution Point*







Enabling Change Management

- `sudo mkdir /mnt/jss_logs`
- `sudo chown -R tomcat7:tomcat7 /mnt/jss_logs`
- Enable change management by going to *Settings* > *General Settings* > *Change Management*
  - Type /mnt/jss_logs into the *Log Directory* field

Change Management

The JSS can be configured to log all changes to a log file or a Syslog server.

Enable Change Management

Log Directory: /mnt/jss_logs

Size of Log File (MB): 20

Syslog Daemon Definitions

Hostname:

Port (Default is 514): 514

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Production Experiences

and lessons learned

- Large downloads over the WAN connection can be painfully slow
  - To offset this, set up one or more local distribution points
    - Use rsync and cron/launchD to keep the distribution points in sync

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Production Experiences, cont.

- Uploading large Packages using Casper Admin can also be very slow if the EC2 distribution point is set as the primary
  - Specify a local distribution point as the primary, then rely on automatic syncing so you're not staring at a progress bar

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Production Experiences, cont.

- Network Segments are your friend
- If your JSS is *puppetized*, make sure it doesn't `ensure => apache_is_absent`
  - This really happened to us :)

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Challenges

What problems did we face?

- curl/libcurl madness
  - HTTPS downloads failing due to a curl/libcurl version mismatch
    - `curl -vv -u casperinstall:pass https://jss.example.com/CasperShare/Packages/test.dmg > ~/Desktop/test.dmg`
    - The above didn't work when testing, but why?...

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Challenges

- `curl -vv -3 -u casperinstall:pass https://jss.example.com/CasperShare/Packages/test.dmg > ~/Desktop/test.dmg`
  - Why did this work?
  - ...because the -3 flag forces curl to use SSLv3 when negotiating with a remote SSL server
  - But why do I need to force it to use SSLv3, shouldn't it be using TLS?...

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Challenges

- **Explanation:** “libcurl linked against OpenSSL 0.9.8* connects to Apache running mod_ssl linked against OpenSSL 1.0.* **AND** there is a mismatch between the hostname in the client request and/or the Common Name (CN) in the SSL certificate and/or the ServerName in the Apache config **THEN** during the initial SSL handshake which determines SSL protocol version, OpenSSL returns a TLS Alert Warning about this mismatch **AND** libcurl interprets this as a fatal error and aborts the connection”
- http://bryanfullerton.com/2013/03/04/git-and-libcurl-with-older-openssl-connecting-to-newer-openssl-error-1112/

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Challenges, cont.

- Using the standard SSL port for Tomcat (443) and 8443 for Apache, (because some people cringe when they see :port suffixes in URLs)
  - Change the `tomcatuser` variable from `tomcat7` to `root` in `/etc/init.d/jamf.tomcat7`
  - Change the `redirectPort` in `/usr/local/jss/tomcat/conf/server.xml` from 8443 to 443
  - `/etc/init.d/jamf.tomcat7 restart`
  - Test connectivity to https://jss001.ec2.example.com/ in a browser

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

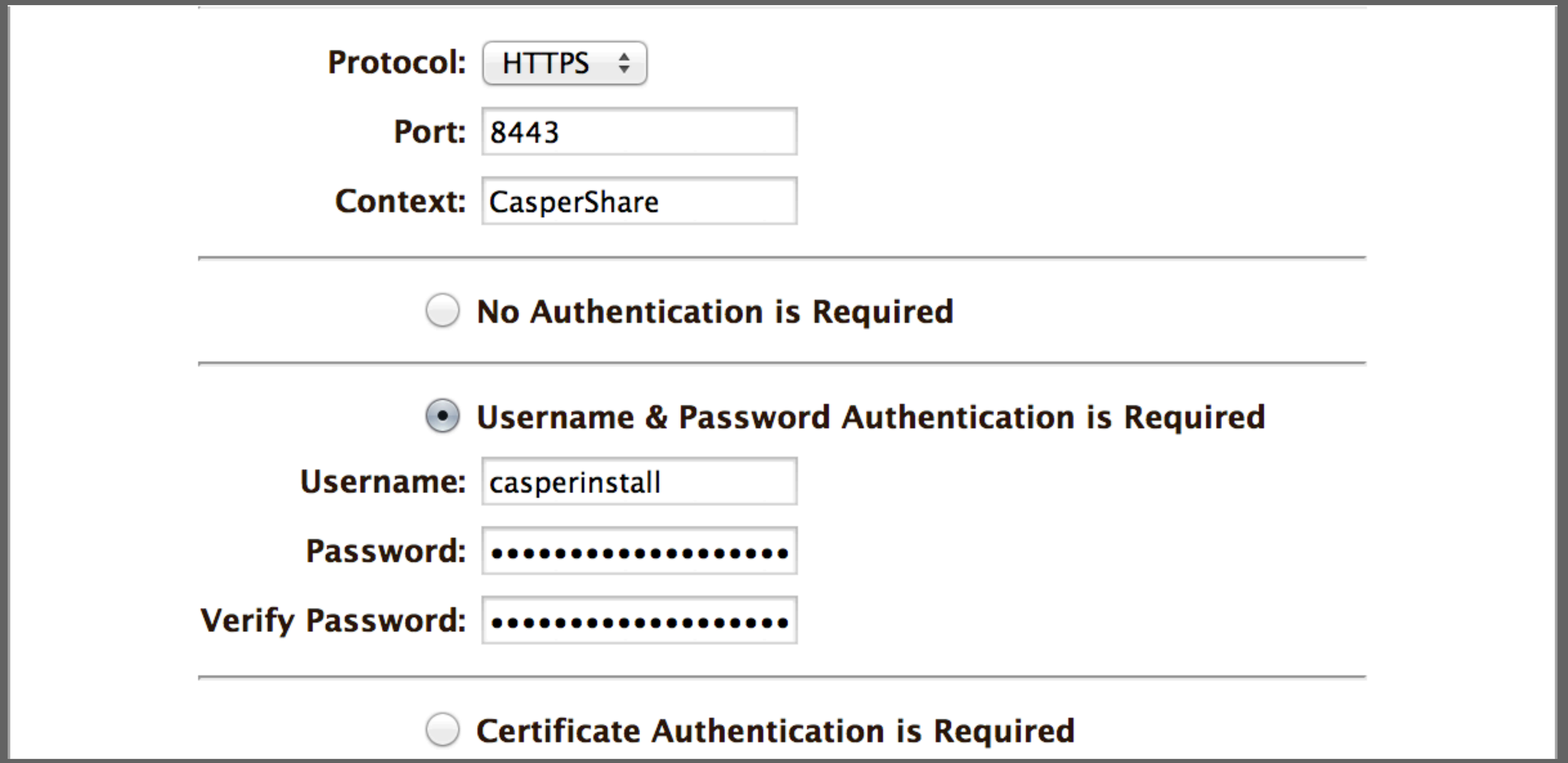
Terminator — vim — ttys009 — 109×24 —

```
 1 <Connector port="443" executor="tomcatThreadPool" SSLEnabled="true" maxHttpHeaderSize="8192"
   maxPostSize="0" maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
   disableUploadTimeout="true" acceptCount="100" scheme="https" protocol="HTTP/1.1" secure="true"
   clientAuth="false" sslProtocol="TLS" keystoreFile="/usr/local/jss/tomcat/.keystore"
   keystorePass="87460176962105803 89" ciphers="SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA,
   TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
   SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA">
~
~
~
~
~
~
~
~
~
~
~
~
~
~
server.xml                                                    1,1           All
"server.xml" [New] 1L, 665C written
```

JAMF NATION user conference

Challenges, cont.

- `sudo vi /etc/apache2/ports.conf`
  - Change Listen from 443 to 8443
- In `/etc/apache2/sites-available/CasperShare-ssl` change the VirtualHost directive to `*:8443`
- `sudo service apache2 restart`
- Remove the port suffix from the JSS URL in *Global Management Framework Settings*
- Specify port 8443 in *Settings* > *Servers* > *Distribution Points*
- Test HTTPS downloads in a browser by going to https://jss001.ec2.example.com:8443/CasperShare/



Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Limitations

What will you be giving up?

- No Casper Remote
  - Clients report a public IP when they're behind a NAT device
- EC2 instance storage is volatile
  - Use EBS (Elastic Block Store) volumes for persistent storage

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

Resources

- http://aws.amazon.com/documentation/
- http://bryanfullerton.com/2013/03/04/git-and-libcurl-with-older-openssl-connecting-to-newer-openssl-error-1112/
- http://www.justinrummel.com/jamf-software-casper-suite-in-an-amazon-ec2-cloud/
- http://www.jamfsoftware.com/sites/default/files/Casper_Suite-9.0_JSS_Installation_Guide_for_Linux.pdf
- http://74bit.com/gossip/2012/09/casper-suite-distribution-point-on-linux/

Linde Group
Technology ▪ Strategy ▪ Integrity

JAMF software

https://github.com/futureimperfect/slides

JAMF NATION user conference

Grazie!

Obrigado!

Danke!

谢谢

Thank you!

Merci!

Gracias!

спасибо!