Certificate Revocation Checking using OCSP and CRL in View 4.5
Table of Contents

Introduction .............................................................................................................................................. 2
About View .................................................................................................................................................. 2
About Smart Card Certificate authentication .......................................................................................... 2
  Smart Card Authentication Infrastructure requirements ................................................................. 2
Brief on Revocation ................................................................................................................................ 3
Certificate Revocation List (CRL) .......................................................................................................... 3
Online Certificate Status Protocol (OCSP) ............................................................................................. 3
Configuring View for Certificate Authentication and Revocation Checking ........................................ 4
Configuring View for Smart Card Authentication ................................................................................. 4
Using / Configuring Certificate Revocation Checking in View ............................................................ 4
  Revocation checking with CRL ............................................................................................................. 4
  Revocation checking with OCSP .......................................................................................................... 5
  OCSP Update Intervals .......................................................................................................................... 5
  Revocation checking with both CRL and OCSP .................................................................................. 6
OCSP/CRL Revocation Checking with Local Mode ............................................................................. 7
  Online-Session (Client and Connection Server can communicate) .................................................... 7
  Offline-Session (Client and Connection Server cannot communicate) ............................................. 7
Tips and Tricks .......................................................................................................................................... 8
  Cross-forest certificate enrollment with Windows Server 2008 ....................................................... 8
  Configuring View to use Http Proxy ................................................................................................... 8
Basic Troubleshooting ............................................................................................................................ 9
About the Authors .................................................................................................................................... 9
Introduction

About View

VMware View is a top-in-class enterprise ‘Desktop Virtualization’ platform. View solution separates the personal desktop environment from Physical system by moving the desktops to a data center and then accessing the desktops using a client-server computing model. VMware View satisfies a rich-set of features required for any Enterprise deployments by providing a robust platform for hosting virtual desktops VMware vSphere. Added to this, capabilities like distributed infrastructure services, failover and recovery of virtual desktops make it a perfect solution.

VMware View provides different authentication mechanisms like Username-password, Smart Card or RSA and further enhancements like Single sign-on (SSO) and Triple SSO. With version 4.5, the Smart-Card authentication has additional manageability with the introduction of OCSP and CRL features. This paper provides technical overview of these features in addition to the specific configurations required in common implementations. Overall, this paper covers:

- Brief on Smart-Card Certificate Authentication
- Brief on OCSP / CRL features
- View Integration with OCSP / CRL
- Some Tips & Tricks
- Basic troubleshooting

About Smart Card Certificate authentication

Smart-Card Certificate Authentication is used by many enterprises as a Security measure. Smart Card Authentication is one of the widely used two-factor authentication mechanisms. Common implementations of two-factor authentication use ‘something you know’ as one of the two factors, and ‘something you have’ as the other factor. A common example of TFA is a bank card (credit card, debit card); the card itself is the physical item, and the personal identification number (PIN) is the data that goes with it.

Smart Card Authentication Infrastructure requirements

The following pre-requisites should be appropriately configured for successful Smart Card Authentication

  - Configure Certificate Authority (CA) to issue the proper certificates.
  - Specify policy that dictates which users can enroll for those certificates.
- Enrollment Agent - This role should be configured in a CA or it can be on a dedicated system. This role is required for enrolling user certificates to smart card.
- Smart Card - Generally a plastic card with embedded Integrated Circuits (ex. Credit Card).
- Smart Card Reader – It is a communication medium between the Smart Card and the Host.
- Cryptographic Service Provider (CSP) drivers – act as an interface to the Smart Card (ex. Microsoft CSP)

For further information on enrolling user certificates on to smart cards, refer http://technet.microsoft.com/en-us/library/cc736901%28WS.10%29.aspx.
Brief on Revocation

Generally, Certificates are issued for a definite lifetime, defined by validity which includes start time and an explicit expiration date. This effectively means the certificate can be issued with a validity of one day, one year or several years. Once issued, a certificate becomes valid from the beginning of its validity time, and it is considered valid until its expiration date is reached. Apart from this, there can be different scenarios which cause a certificate to become invalid prior to expiration. Certificates are often revoked when a user leaves an organization, loses a smartcard, or moves from one department to another.

To enable revocation, RFC 5280 lists the following different states that can be applied by a CA on any of its issued certificates.

<table>
<thead>
<tr>
<th>CRL REASON</th>
<th>REASON CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>0</td>
</tr>
<tr>
<td>keyCompromise</td>
<td>1</td>
</tr>
<tr>
<td>cACompromise</td>
<td>2</td>
</tr>
<tr>
<td>affiliationChanged</td>
<td>3</td>
</tr>
<tr>
<td>Superseded</td>
<td>4</td>
</tr>
<tr>
<td>cessationOfOperation</td>
<td>5</td>
</tr>
<tr>
<td>certificateHold</td>
<td>6</td>
</tr>
<tr>
<td>Not Used</td>
<td>7</td>
</tr>
<tr>
<td>removeFromCRL</td>
<td>8</td>
</tr>
<tr>
<td>privilegeWithdrawn</td>
<td>9</td>
</tr>
<tr>
<td>aACompromise</td>
<td>10</td>
</tr>
</tbody>
</table>

There are two popular certificate validation mechanisms, which are:

- **CRL** - Certificate Revocation List
- **OCSP** - Online Certificate Status Protocol

**Certificate Revocation List (CRL)**

A digitally signed list issued by a CA that contains certificates that have been revoked. The list includes the serial number of the certificate, the date certificate was revoked, and the revocation reason. View Connection Server can perform CRL checking to determine a presented certificate's revocation status. There are two variants of CRL, they are:

- **Base/Full CRL**: A type of CRL that contains list of certificates revoked and published automatically in specified intervals as defined by the administrator of CA.
- **Delta CRL**: A type of CRL that contains list of certificates revoked since the last base/full CRL was published.

**Online Certificate Status Protocol (OCSP)**

OCSP is a protocol which supplements CRL validation. It allows high-performance validation of certificate status. Further, OCSP Server can retrieve the CRLs from all the CAs in an Organization. Upon
OCSP server can act as a single point of contact for revocation validation of the entire Organization, by allowing client applications to obtain timely information on revocation status of a certificate.

OCSP Server works using Responder-Repeater configuration. Typically, an Enterprise would have a single Responder and multiple Repeaters configured.

### Configuring View for Certificate Authentication and Revocation Checking

#### Configuring View for Smart Card Authentication

The following steps are required for Smart Card authentication in View.

- Obtain Root certificate from Certificate Authority
- Create trust store using keytool
- Create locked.properties file with appropriate attributes

For further details regarding the configuration of Smart card Authentication with respect to VMware View, refer VMware View 4.5 Admin Guide.

#### Using / Configuring Certificate Revocation Checking in View

View supports revocation checking with Certificate Revocation Lists (CRLs) as well as Online Certificate Status Protocol (OCSP) for Connection Server and Security Server instances. Both CRL and OCSP features can be configured on a Single Server (Standard, Replica, Security) instance. When both types of certificate revocation checking mechanism are configured, View attempts to use OCSP in first instance and falls back to CRL on OCSP failure. However, please note that View does not fall back to OCSP if CRL fails.

For further details regarding the configuration of Certification Revocation Lists (CRLs) and OCSPs with respect to VMware View, refer VMware View 4.5 Admin Guide.

#### Revocation checking with CRL

When View is configured for revocation checking with CRL, the revocation status of a certificate is determined by accessing the CRL published by appropriate CA. If a certificate is found to be revoked, View client throws an appropriate error "Smart card Authentication failed. Please contact your Administrator. (Revocation Checks failed)."

Once With respect to the CRL configuration to integrate it with View, the steps mentioned under the section Configuring View for Smart Card Authentication need to be followed. Once these steps are carried out successfully, the locked.properties file needs to be added with updated appropriate attribute values.

The following attribute values in the locked.properties file are mandatory for View to be configured to use CRL revocation checking.

```plaintext
trustKeyfile=longa.key
trustStoretype=JKS
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

Once the above attributes are configured, restart the View Connection Server service for the changes to take effect.
Revocation checking with OCSP

When View is configured for revocation checking with OCSP, the revocation status of a certificate is determined by sending a verification request to an OCSP Responder. If a certificate is found to be revoked, View client throws appropriate error message.

Clockwise from left: 1. View Client prompts user to select a certificate from the list of available certificates; 2. User prompted for PIN entry; 3. Error message stating certificate revocation

The following attribute values in the locked.properties file are mandatory for View to be configured to use OCSP revocation checking.

- trustKeyfile=lonqa.key
- trustStoretype=JKS
- useCertAuth=true
- enableRevocationChecking=true
- enableOCSP=true
- allowCertCRLs=true
- ocspSigningCert=te-ca.signing.cer
- ocspURL=http://te-ca.lonqa.int/ocsp

OCSP Responder signing certificate needs to be placed alongside the locked.properties file and its name should be specified under the attribute ocspSigningCert.

Once the above attributes are configured, restart the View Connection Server service for the changes to take effect.

**OCSP Update Intervals**

CA publishes CRLs at regular intervals based on the configuration. However, OCSP Responder can be configured to refresh its revocation lists based on either the validity period of the CRL being used, or at a manually configured interval.
Windows 2008 Server can be configured as an OCSP Responder. For detailed instructions on setting up and configuring OCSP, refer to Microsoft TechNet

**Revocation checking with both CRL and OCSP**

VMware View can be configured to use both CRL and OCSP mechanisms together. The following attribute values in the locked.properties file are mandatory for View to be configured to use both CRL and OCSP revocation checking together.

- trustKeyfile=lonqa.key
- trustStoretype=JKS
- useCertAuth=true
- enableRevocationChecking=true
- enableOCSP=true
- ocspCRLFailover=true
- allowCertCRLs=true
- ocspSigningCert=te-ca.signing.cer
- ocspURL=http://te-ca.lonqa.int/ocsp
- crlLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl

When both CRL and OCSP are configured, OCSP will have higher priority over CRL revocation checking. In such a configuration if OCSP validation fails, then View will fall-back to CRL validation. This fall-back mechanism is controlled by the attribute `ocspCRLFailover` in `locked.properties` file.

Once the above attributes are configured, restart the View Connection Server service for the changes to take effect.

A pictorial representation of View integration with OCSP Responder
VMware View admin UI provides various options for Smart card authentication. These are:

- Optional: If 'Smart Card authentication' is set to optional, user is allowed to login using username/password on smart card authentication failure.
- Required: If 'Smart Card authentication' is set to required, user is NOT allowed to login using username/password on smart card authentication failure.
- Not allowed: If 'Smart Card authentication' is set to Not allowed, user is NOT allowed to login using a smart card.

The below figure illustrates this:

OCSP/CRL Revocation Checking with Local Mode

There are two scenarios possible with Local Mode authentication

**Online-Session (Client and Connection Server can communicate)**
Certificate revocation checking is performed as in a normal remote session; as under:

- User Certificate is un-revoked: If the user certificate is not revoked, the authentication succeeds.
- User Certificate is revoked: If the user certificate is revoked, the authentication fails.

**Offline-Session (Client and Connection Server cannot communicate)**
The prerequisite which is assumed here is that the View Connection Server is online and the Checked out desktop can contact the View Connection Server.
Tips and Tricks

Cross-forest certificate enrollment with Windows Server 2008

Traditionally, an enterprise Certification Authority (CA) is limited to issuing certificates only to the clients that belong to the same Active Directory (AD) forest. This means that, user and client computers would only attempt to enroll certificates from a CA in its local forest, especially in auto enrollment scenarios. Further this drawback forces administrators to have at least one CA per Forest.

Starting with Windows Server 2008 R2, this barrier is removed by supporting cross-forest certificate enrollment. This feature allows clients to enroll for a certificate from a CA of a different AD forest further reducing the number of CAs in a multi-forest environment.

For further details regarding the cross-forest certificate enrollment, refer to Microsoft Whitepaper

Configuring View to use Http Proxy

If there is no proxy server configured in a company’s environment, this step can be safely skipped.

There are instances where Enterprises would have revocation checking mechanisms placed outside a company’s internal network. In such cases, the View Connection Server needs to contact an entity outside the internal network. If the Company has a policy to direct Internet traffic through Proxy then View connection server requires additional configuration to contact OCSP Responder. This is because the View Server uses Java socket which doesn’t depend on IE proxy settings.

Following steps illustrates the procedure to setup the View Java Socket Layer for the Proxy settings:

- Open the Registry Hive

\HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params

- Configure ‘Dhttp.proxyHost’ and ‘Dhttp.proxyPort’ keys. For example: -

  Dhttp.proxyHost=<proxy123>
  Dhttp.proxyPort=<proxyport>

Note: These values need to be appended and should not overwrite the previous values.

- Restart the Connection Server Service for the Changes to take effect.

The above steps configures Java socket used by the View Server to use proxy for https requests enabling View Server to contact OCSP Responder.
Basic Troubleshooting

- Driver related issues: Ensure proper drivers are in-place for Smart card readers, Smart cards on both Client and Agent machines.
- Misconfigurations in locked.properties file: Ensure all entries in the locked.properties file are syntactically correct. Refer VMware View 4.5 Admin Guide for correct syntax.
- Ensure creation of truststore files with valid and appropriate Root CA Certificate.
- Ensure View Server can contact OCSP Responder by accessing the URL specified in locked.properties
- Ensure OCSP Responder signing certificate is valid.
- Ensure OCSP Responder can communicate to CA infrastructure

About the Authors

Raghavendra Babu is a QE Manager in VMware. He has been leading View Core QA efforts from Bangalore. He has a BE in Computer Science and his previous experience includes companies like Dell India R&D, Quark etc.

Noble Peter is a Software QE Engineer in VMware. He is part of the View Core QA team in Bangalore. He has a MSc in DDES from Manipal University.

Suhas Hariharan is a Software QE Engineer in VMware. He is part of the View Core QA team in Bangalore. He has an MTech in Computer Science from Manipal University.