Abstract

This guide describes required components and configuration steps for deploying RSA SecurID® two-factor authentication in the VSPEX Citrix XenDesktop end user computing proven infrastructures. This guide and its associated Implementation Guide are designed to be used as additions, or “overlays,” to one of the specific VSPEX View proven infrastructures documents.

January, 2013
Contents

Chapter 1 Introduction
Purpose
Business value
Scope
Audience

Chapter 2 Solution Overview
Key components
Existing infrastructure
RSA SecurID with Authentication Manager
Citrix NetScaler
Citrix Storefront
EMC VSPEX
Virtual machine requirements and profile
Sizing and scaling information for RSA Authentication Manager
Sizing and scaling information for Citrix NetScaler VPX
Sizing and scaling information for Citrix Storefront
High-level solution architecture
Architecture overview

Chapter 3 Before You Start
Prerequisites
Allocate compute, memory, and storage resources
Acquire software and licenses
Allocate required IP Addresses, create DNS entries
Acquire SSL certificates
Create four Windows Server 2008 R2 guests
Support resources

Chapter 4 Solution Implementation
Server and virtualization implementation
Design considerations
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application implementation.................................................................. 26</td>
</tr>
<tr>
<td>Install and configure RSA Authentication Manager............................. 26</td>
</tr>
<tr>
<td>Install and configure Citrix NetScaler VPX..................................... 29</td>
</tr>
<tr>
<td>Install and configure Citrix Storefront........................................ 34</td>
</tr>
<tr>
<td>Backup and recovery implementation.................................................. 37</td>
</tr>
<tr>
<td>RSA Authentication Manager.................................................................. 37</td>
</tr>
<tr>
<td>Citrix NetScaler VPX, Citrix Storefront........................................... 37</td>
</tr>
<tr>
<td>Chapter 5 Solution Validation............................................................ 39</td>
</tr>
<tr>
<td>Baseline hardware validation............................................................... 40</td>
</tr>
<tr>
<td>RSA SecurID functional validation...................................................... 40</td>
</tr>
<tr>
<td>Verifying external network access...................................................... 41</td>
</tr>
<tr>
<td>Verifying local network access........................................................... 43</td>
</tr>
<tr>
<td>Functional validation methodology...................................................... 44</td>
</tr>
<tr>
<td>Key metrics......................................................................................... 44</td>
</tr>
<tr>
<td>Define the test scenarios..................................................................... 44</td>
</tr>
<tr>
<td>Chapter 6 Reference Documentation.................................................... 47</td>
</tr>
<tr>
<td>White papers......................................................................................... 48</td>
</tr>
<tr>
<td>Product documentation........................................................................... 48</td>
</tr>
<tr>
<td>Other documentation............................................................................. 48</td>
</tr>
<tr>
<td>Appendix A Configuration Information................................................ 49</td>
</tr>
<tr>
<td>Table of required configuration information....................................... 50</td>
</tr>
</tbody>
</table>
Figures

Figure 1. Logical architecture: generalized VSPEX Citrix XenDesktop proven infrastructure with RSA SecurID, Citrix NetScaler, and Citrix Storefront components overlaid in a redundant configuration.......................... 17
Figure 2. Default Access Gateway login dialog .............................................. 41
Figure 3. Browser-based Citrix Receiver client – automatic login to virtual desktop in progress ........................................................................................................... 42
Figure 4. Browser-based Citrix Receiver client – Active Directory login challenge 43
Figures
### Tables

Table 1. Baseline compute and storage requirements for SecurID overlay ........ 15  
Table 2. Required configuration information for RSA Authentication Manager ... 50  
Table 3. Required configuration information for Citrix NetScaler VPX ............. 50  
Table 4. Required configuration information for Access Gateway Virtual Server 51  
Table 5. Required configuration information for NetScaler Load Balancers .... 51  
Table 6. Required configuration information for Storefront .......................... 51
This chapter presents the following topics:

Purpose ........................................................................................................................................... 10
Business value ................................................................................................................................. 10
Scope ............................................................................................................................................... 11
Audience ........................................................................................................................................ 11
Purpose

This document describes infrastructure components required and a configuration framework for deployment of RSA SecurID two-factor authentication in a new or existing VSPEX Citrix XenDesktop end user computing infrastructure.

EMC VSPEX End-User Computing Solutions for Citrix XenDesktop and VMware vSphere provide proven, best-of-breed solutions for end user computing. Customers requiring additional access protection for remotely-available or sensitive XenDesktop environments can enable RSA SecurID two-factor authentication as a highly-effective additional layer of virtual desktop access protection. In addition to Active Directory credentials, accessing a SecurID-protected resource requires a personal identification number and a constantly-changing code from a hardware or software-based “token”. Credentials based on something the user knows (the PIN) and something the user has (the token code) is the basis of two-factor authentication and is a standard in access security.

The following components are used to implement SecurID in the VSPEX XenDesktop infrastructures:

- RSA Authentication Manager (version 7.1 SP4 or higher)
- Citrix NetScaler network appliance (version 10 or higher)
- Citrix Storefront (version 1.2, also known as CloudGateway Express)

RSA Authentication Manager manages SecurID hardware or software tokens and their assignment to users as well as the actual authentication process. For this design, Authentication Manager uses Active Directory as its source of users (“identity store”).

Citrix NetScaler enables seamless integration of RSA SecurID functionality into the VSPEX XenDesktop environment as well as provision of enhanced management and availability features and a streamlined user experience. Citrix Storefront provides a set of service interfaces used by NetScaler and Citrix clients to access XenDesktop.

It is important to note that the NetScaler and Storefront configuration used in this design is only one of many possible usage scenarios. These components offer a tremendous amount of additional functionality well beyond the scope of this solution; they are used here to support the primary goal of adding SecurID authentication to the VSPEX XenDesktop infrastructures. Presence of these components in the environment provides a foundation on which EMC channel partners can build many other service enhancements for the customer.

Business value

As described in their individual infrastructure documentation, VSPEX Citrix XenDesktop end user computing solutions provide predefined infrastructures with proven, tested performance, scalability and functionality for up to 250 desktops (using EMC VNXe storage) or up to 2000 desktops (using EMC VNX storage). This overlay enhances the value proposition by strengthening access security, especially for remote connections.
Introduction

Scope

The access and security enhancements presented in this guide are assembled as an “overlay” to the Citrix XenDesktop VSPEX solutions. This document briefly describes SecurID and Authentication Manager, illustrates their integration into the predefined VSPEX solution, and presents a configuration framework. The overlay is not intended as a standalone solution; infrastructure services built into the VSPEX solutions (notably Active Directory, SQL Server, and DNS) are used to support the extended functionality described here.

This guide is intended to be used in conjunction with the referenced VSPEX Proven Infrastructure documents. Familiarity with the relevant documents is a minimum prerequisite for using this guide.

Audience

This guide is targeted to EMC internal staff and channel partners. It is not intended for external distribution or the VSPEX end users.
Introduction
Chapter 2   Solution Overview

This chapter presents the following topics:

Key components ........................................................... 14
High-level solution architecture ................................... 17
Key components

**Existing infrastructure**

The XenDesktop environment and supporting infrastructure services such as Active Directory and DNS are or should be configured according to the appropriate VSPEX proven infrastructure document. Compute and storage resource for the components described below may be added for the purpose or consumed from the solution pool as described later in this overlay document.

**RSA SecurID with Authentication Manager**

SecurID functionality is managed by RSA Authentication Manager. Many companies deploy SecurID to authenticate access to a corporate network from a connection on a public network. When accessing XenDesktop from a public network, the user is challenged for both SecurID and domain credentials. Upon successful authentication, the user is logged in without further challenge. For XenDesktop access from within the local network, the user is authenticated only at the domain level.

For this overlay, Authentication Manager is installed on redundant Windows Server 2008 R2 virtual servers. While both nodes are active, the Citrix NetScaler appliance (described below) will direct traffic to a single node as long as that “primary” node is responsive; in the event of primary node failure, NetScaler will utilize the secondary node until the primary returns to operational status. Built-in Authentication Manager features provide backup and synchronization services.

Note: Authentication Manager 7.1 is also available as a physical appliance.

A RADIUS server is configured on each Authentication Manager node to listen for and process SecurID requests arriving from NetScaler's Access Gateway; native RSA authentication is not supported by this edition. RADIUS does not require RSA Authentication Agent software to be installed on the protected XenDesktop hosts. Note that NetScaler Access Gateway is explicitly registered as an Authentication Client during RADIUS setup.

**Citrix NetScaler**

Citrix NetScaler is a highly versatile network appliance which can deliver a variety of cloud control services such as data compression, content caching, load balancing, application acceleration, etc. Deployed in the network demilitarized zone (DMZ), NetScaler’s Access Gateway Enterprise Edition (AGEE) provides secure access to XenDesktop and other resources within the secure network from external or public networks. AEGE is used in this solution to control primary (SecurID) and secondary (Active Directory) authentication for users accessing XenDesktop outside the secure network.

NetScaler’s load balancing capabilities are used to provide High Availability (HA) as well as load-balanced access to redundant Citrix Storefront instances.

**Citrix Storefront**

Storefront, also known as Citrix CloudGateway Express, provides authentication and desktop delivery services for web and mobile versions of the Citrix client. For access attempts from Microsoft Windows or Apple Mac OS X, Storefront facilitates the download and installation of Citrix Receiver if the client is not already installed. After validating a user’s credentials, the Storefront authentication service ensures that all subsequent interactions are processed without repeating the logon sequence. Storefront then records details of the application subscription and associated...
shortcuts and locations, enabling a consistent user experience across sessions and devices.

**EMC VSPEX**

VSPEX validated and modular architectures are built with proven best-of-breed technologies to create complete virtualization solutions that enable you to make an informed decision in the hypervisor, compute and networking layers. VSPEX eliminates desktop virtualization planning and configuration burdens. VSPEX accelerates your IT Transformation by enabling faster deployments, greater choice, efficiency, and lower risk.

Authentication Manager, NetScaler, and Storefront can be hosted on new VMware ESXi hardware dedicated to the purpose or on existing infrastructure servers described in appropriate reference architectures if capacity is sufficient. Refer to the VSPEX View virtual infrastructure document for hardware requirement information, which defines a standard “reference virtual machine.”

In order to maintain high availability, ensure that VMware guests running nodes of redundant pairs are placed on separate physical servers.

Table 1 shows minimum CPU, memory, and disk space values for VMware guests hosting Authentication Manager, NetScaler VPX, and Storefront. Large or high-traffic deployments may require additional resource, especially for NetScaler. EMC channel partners should work with customers to ascertain throughput requirements in order to ensure adequate capacity.

**Table 1. Baseline compute and storage requirements for SecurID overlay**

<table>
<thead>
<tr>
<th></th>
<th>CPU (cores)</th>
<th>Memory (GB)</th>
<th>Disk (GB)</th>
<th>SQL Database*</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Authentication Manager</td>
<td>2</td>
<td>8**</td>
<td>60</td>
<td>n/a</td>
<td>RSA Authentication Manager 7.1 Performance and Scalability Guide</td>
</tr>
<tr>
<td>Citrix NetScaler</td>
<td>2</td>
<td>4</td>
<td>40</td>
<td>n/a</td>
<td>Citrix NetScaler VPX Getting Started Guide</td>
</tr>
<tr>
<td>Citrix Storefront</td>
<td>2</td>
<td>2</td>
<td>20</td>
<td>3.5 MB per 100 users</td>
<td></td>
</tr>
</tbody>
</table>

* It is expected that this capacity can be drawn from existing SQL Server defined in the VSPEX Citrix XenDesktop reference architectures.

** RSA recommends an 8GB minimum for VMware-based deployments. A 4 GB or even 2 GB configuration is acceptable on standalone servers.**
The installation used in this overlay places Authentication Manager and associated RADIUS server on the same host.

According to the RSA Authentication Manager 7.1 Performance and Scalability Guide, a small current-generation server with a single dual-core processor and 2GB RAM can process 40 SecurID authentications per second. Thus, an entire user database for a 2,000 desktop VSPEx environment can be authenticated in under a minute (RSA testing performed on dedicated hardware with no antivirus, security, or other software installed).

**NOTE** Deployment of Authentication Manager on VMware guests carries specific requirements and restrictions.

- Allocated memory should be set to 8GB for 64-bit operating systems
- Cloning, physical-to-virtual conversion, and virtual-to-physical conversion are supported.
- Snapshots, vMotion, High Availability, and several other VMware virtualization features are not supported. RSA recommends that Authentication Manager built-in features be used for these types of services.

See release notes for Authentication Manager 7.1 SP4 (available on RSA SecurCare Online) for more information.

This overlay uses the NetScaler virtual appliance (VPX), a lower-cost solution targeting toward the SMB customer as compared to the enterprise-oriented physical appliance series.

The most likely bottleneck to be encountered with a VPX in the overlay environment is network bandwidth. A throughput baseline of 150 kbs per session can be used for sizing approximation; environments supporting heavy multimedia use can consume 600 kbs. Consult NetScaler sizing documentation for guidance on insuring adequate capacity.

Storefront server requirements are satisfied by the standard infrastructure server footprint described in the relevant proven infrastructure documents.

Storage requirements for Storefront’s SQL Server subscription database are minimal. The database stores information allowing a consistent user experience across multiple sessions and client devices; browser-based access generates no database entry at all.
High-level solution architecture

Figure 1 shows the generalized logical architecture of the VSPEX Citrix XenDesktop infrastructure, with the overlay infrastructure added. The VNX with Fibre Channel variant is shown. NFS and VNXe variants are described in the Citrix XenDesktop VSPEX proven infrastructure documents.

Note While this diagram shows SecurID infrastructure hosted on separate vSphere servers for clarity, these components may be placed on existing infrastructure hosts if sufficient capacity is available. See Table 1 on page 17.

Figure 1. Logical architecture: generalized VSPEX Citrix XenDesktop proven infrastructure with RSA SecurID, Citrix NetScaler, and Citrix Storefront components overlaid in a redundant configuration.

Architecture overview

The SecurID overlay architecture consists of the following components.

EMC VSPEX End-User Computing: Citrix XenDesktop 5.6 and VMware vSphere 5.1 for up to [250 or 2000] Virtual Desktops — The foundation infrastructure supports XenDesktop and provides Active Directory, DNS, and SQL Server services, which are also utilized by the overlay.
RSA Authentication Manager 7.1 SP4 – In addition to managing SecurID token assignment to users, Authentication Manager controls the RADIUS server which listens for incoming authentication requests. Authentication Manager is deployed on redundant nodes for high availability. The following configuration notes are important:

- The solution overlay described here uses Citrix Access Gateway Enterprise Edition (AGEE), which is incorporated with Citrix NetScaler 10 (described below). AGEE only supports SecurID authentication via RADIUS. While out of scope for this overlay, it should be noted that the (standalone) Standard and Advanced editions of Access Gateway must use the native RSA authentication API. Citrix Secure Gateway is not supported.

- Authentication Manager's installation wizard provides easy setup of primary and secondary nodes. After setup, both nodes are active and equal; the primary-secondary relationship refers to synchronization: changes are made to the primary nodes, and are then ported to the secondary.
  - While the secondary Authentication Manager node is easily synchronized with the primary, a RADIUS server must be manually configured on the secondary: the sync process will not port the server setup.
  - Duplicate NetScaler AGEE policies are required for high availability, as described below.

Citrix NetScaler 10 network appliance – While NetScaler offers a wide variety of functionality to control and accelerate network services and cloud-based applications, two primary subcomponents are used in this overlay.

- Access Gateway Enterprise Edition (AGEE) – Deployed in the network DMZ, AGEE provides a gateway for external traffic to access XenDesktop resources on a protected network. Users enter credentials in a single authentication dialog, and AGEE policies control primary authentication against RSA SecurID and secondary authentication against Active Directory.

  Note For this solution, the primary authentication policy is actually comprised of duplicate SecurID authentication policies supporting high availability:
  - The first SecurID policy points to the primary Authentication Manager node.
  - The second SecurID policy is identical to the first, but with a lower priority setting, and points to the secondary AM node. If the primary node becomes unreachable, AGEE detects the first policy execution failure and runs the second policy.

- Load Balancing – Virtual load balancers are configured to provide high availability access to Citrix Storefront’s redundant nodes. A secondary Storefront host does not have the capability of listening for requests sent to a failed primary; therefore, NetScaler load balancing is configured to monitor Storefront node availability and route requests accordingly.

NetScaler is deployed in this solution as an active-passive pair. If the primary becomes unreachable, the secondary automatically takes over and services all traffic.
that was explicitly destined for the primary instance. In this configuration, only the active instance services traffic. While NetScaler supports clustering, wherein both instances serve traffic at the expense of increased configuration and network overhead, the Access Gateway subcomponent is not supported in that configuration.

NetScaler is available as a physical appliance or downloadable VMware OVF file, which can be quickly and easily loaded onto a VMware vSphere host as a virtual appliance (VPX). Configuration and management are identical, although VPXs are more limited in scalability. Licensing determines which capabilities are enabled on the appliances and at what service levels.

Customer consultation to ascertain traffic load and appropriate NetScaler model is strongly advised.

**Citrix Storefront 1.2** - Storefront is the replacement for Citrix Web Interface. In this solution, Storefront’s primary purposes are to:

- Present user desktops to web-based or mobile Citrix client,
- Provide authentication services for local-network user access,
- Simplify internal / external access configuration in the XenDesktop environment.

User subscription information, stored in a backend SQL Server database, provides consistent desktop or other application experience across user sessions and differing client devices.

**Citrix Receiver** – Software client providing optimal access to XenDesktop and other Citrix published resources. The client is available for most mobile devices; for Windows and Mac OS X, the user will be prompted for automatic download and installation of the client on first browser access of the environment. In this proven infrastructure, the user client is considered a generic user endpoint, so versions of the Receiver client and options and optimizations for them are not addressed.
Chapter 3  Before You Start

This chapter presents the following topics:

Prerequisites .................................................................................................................. 22
Support resources .......................................................................................................... 23
Before You Start

Prerequisites

Steps in this guide are targeted for an existing VSPEX VMware View end user computing infrastructure, as described in the following documents:

- **EMC VSPEX End-User Computing: Citrix XenDesktop 5.6 and VMware vSphere 5.1 for up to 250 Virtual Desktops, Enabled by EMC VNXe and EMC Next Generation Backup**

- **EMC VSPEX End-User Computing: Citrix XenDesktop 5.6 and VMware vSphere 5.1 for up to 2000 Virtual Desktops, Enabled by EMC VNX and EMC Next Generation Backup**

Complete the following steps should be before installation.

Allocate compute, memory, and storage resources

Refer to Table 1 for guidance on resource provisioning.

It is expected that the Citrix NetScaler virtual appliance (VPX) for VMware, configured as an active-passive pair, will satisfy VSPEX Citrix end user computing throughput requirements. However, channel partners are advised to consult with customers to insure adequate capacity per Citrix guidance.

Acquire software and licenses

The following software and licenses are required:

- RSA Authentication Manager 7.1 SP4 or later (plus sufficient hardware or software tokens): Installation media received or downloaded, and licenses, tokens, token records, and import passwords have been received from RSA

- Citrix NetScaler VPX (version 10 or later, downloadable from the myCitrix portal linked from http://www.citrix.com) with licensing to cover Access Gateway Enterprise Edition and load balancing for the expected number of users.

  **Note** NetScaler licenses require the MAC address of the virtual machine which will run the VPX; this is user-configurable from the vSphere console but should be planned in advance.

- Citrix CloudGateway Storefront 1.2 or later

- Licensing and installation media for four Windows Server 2008 R2 instances

Allocate required IP Addresses, create DNS entries

Use the tables in Appendix to plan and record naming and network information for:

- Authentication Manager Hosts 1 and 2
- Storefront Hosts 1 and 2
- NetScaler Appliances 1 and 2 Management IPs (NSIP)
- NetScaler Appliances 1 and 2 Mapped IPs (MIP) for initial setup
- NetScaler Appliance Mapped IP (MIP) for initial setup
- NetScaler load balancing Virtual server IP (VIP) for internal VDI access
- NetScaler load balancing Virtual server IP (VIP) for external VDI access
Before You Start

- NetScaler Access Gateway Virtual Server IP (VIP) for external VDI access
- NetScaler load balancer virtual server for internal MIP

Acquire SSL certificates

SSL certificates are required for:

- RSA Authentication Manager servers (two).
  Refer to “Managing Certificates and Keystores for SSL” in the RSA Authentication Manager Installation and Configuration Guide for instructions to generate and assign SSL certificates for Authentication Manager.

- Citrix NetScaler virtual appliance (two), Citrix NetScaler Access Gateway virtual server.
  Steps for generating public SSL certificates for NetScaler are found in Citrix support article CTX109260.

- Citrix Storefront servers (two).
  Citrix Storefront runs on a dedicated instance of IIS 7.5, in turn running on Windows Server 2008 R2. SSL certificates for Storefront are therefore generated for the IIS instance. The certificate request, installation, and bind process for Storefront is described in the Citrix white paper “Citrix CloudGateway Express 2.0 Proof of Concept Implementation Guide.” The paper also serves as the foundation for installing and configuring Storefront.

Since SSL certificates are assigned to a specific Fully Qualified Domain Name (FQDN), it is important to carefully plan naming conventions for physical and virtual servers.

Upon receipt from the issuing Certificate Authority (CA), copy SSL certificates to a location from which they can be easily imported to the target servers, such as a network share or VMware datastore.

Create four Windows Server 2008 R2 guests

These VMs are used for:

- Primary and secondary Authentication Manager nodes
- Primary and secondary Storefront nodes

Each instance should be configured and patched to production standards and joined to the applicable domain.

Support resources

Support of SecurID and Authentication Manager is provided through RSA (http://www.rsa.com).

Support for Citrix NetScaler and Citrix Storefront is provided through Citrix (http://www.citrix.com).
Chapter 4  Solution Implementation

This chapter presents the following topics:

Server and virtualization implementation .................................................. 26
Application implementation ......................................................................... 26
Backup and recovery implementation......................................................... 37
Solution Implementation

Server and virtualization implementation

Design considerations

Deployment of SecurID in the VSPEX XenDesktop infrastructures involves installation and configuration of RSA Authentication Manager, Citrix NetScaler, and Citrix Storefront. Active Directory, DNS, and other infrastructure services supporting XenDesktop will also support Authentication Manager.

This overlay is intended to provide a basic HA Authentication Manager service in the VSPEX XenDesktop environment. Optimization and operational planning (for backup, node synchronization, etc.) are beyond the scope of the guide.

Infrastructure for the SecurID overlay conforms to the design presented in the relevant VSPEX Citrix XenDesktop end user computing infrastructure document. Storage requirements are minimal and expected to be available from the VSPEX pool without additional drives added.

Application implementation

Implementation of the SecurID overlay involves configuration of three major components (RSA Authentication Manager, Citrix NetScaler, and Citrix Storefront), and some of the steps are interdependent. Except as noted, complete setup of all three components before performing any verification steps or addressing error or warning messages.

The steps are performed in the installation wizards of each component in order to remain current as versions change. As wizards progress, use defaults except as noted. Be sure to record all information used, such as IP assignments, IDs and passwords, DNS aliases, etc.

Install and configure RSA Authentication Manager

This section contains steps for setup of a high-availability Authentication Manager 7.1 SP4 installation on Windows Server 2008 R2 virtual machines. The steps provided below compliment, as opposed to echo, the Authentication Manager installation wizard. As the wizard proceeds, use defaults except as noted. Be sure to record all information used, such as IP assignments, IDs and passwords, DNS aliases, etc.

References

- RSA Authentication Manager 7.1 Installation and Configuration Guide
- RSA Authentication Manager 7.1 Administrator’s Guide

Steps

1. Install Authentication Manager 7.1SP4 software on primary host, using IP, DNS, and other network information previously recorded in Appendix .
   a. Map target server access to the installation media.
   b. Place the license files in the same location as media for easy access when prompted.
   c. Start the installation executable (double-click autorun.exe if necessary).

When prompted, provide the following information:
i. **Installation type:** Primary instance

ii. Path to License file folder

iii. RSA Security Console credentials (these are local credentials: RECORD AND STORE IN A SECURE LOCATION)

**Note** The installation triggers creation of a 2048-byte certificate issued by "RSA Authentication Manager Root CA" for the FQDN of the Authentication Manager host.

2. To import Certificate Authority root certificate, select **Deployment Configuration → Certificates → Identity Source Certificates** in the Security Operation Console.

3. To set up Active Directory as identity source, select **Deployment Configuration → Identity Sources → Add New** in the Security Operations Console.

   a. When the wizard prompts for the AD source (Directory URL: field), use ldaps --instead of http or https as the protocol.

   b. In **Directory User ID** field, use fully qualified domain\userid format - wizard will not assume domain.

   c. Sample Active Directory entries:
      i. Directory URL: ldaps://myDomainController.myDomain.com
      ii. User Base DN: cn=Users,dc=myDomain,dc=com
      iii. User Group Base DN: cn=Users,dc=myDomain,dc=com (same as base DN)

   d. Link the new AD identity source to the default (**System Domain**) or custom realm to make AD users available for token assignment dialog. See “Appendix A, Linking an Identity Source to a Realm,” in the **Administrator's Guide** for more information.

      i. Navigate to **Security Console--->Administration--->Realms--->Manage Existing**

      ii. Select the realm

      iii. Select **Edit**

      iv. Follow the instructions in the dialog for other options.

4. Configure a RADIUS server.


   b. Provide the following information. These items are locally stored, so careful recording in **Appendix** table is imperative:

      i. Replication Secret
      ii. Master Password
      iii. Admin User ID
      iv. Administrator Password
5. Configure Citrix NetScaler as the RADIUS Client
   a. In Authentication Manager Security Operations Console, navigate to Deployment Configuration → RADIUS → RADIUS Clients → Add New
      i. Enter data fields (leave it as the default if not specified here):
         (1) Client Name: NetScaler FQDN from Appendix
         (2) IP Address: NetScaler management address (the NSIP address - not Access Gateway address)
         (3) Shared Secret: RADIUS server secret entered above
      ii. Click Save and Create Associated RSA Agent.
         (1) New Authentication Agent screen appears.
         (2) Default values on this screen are acceptable. Click Save.
   b. REPEAT step a for secondary NetScaler - if not done, incoming authentication requests from it will not be answered in event of a NetScaler failover.

6. Generate an Authentication Manager "replica package file" per Chapter 4 of the Installation Guide. Even when Automatic option is selected for how to transfer data, click the link to download and save the .pkg file.

7. Configure a secondary host (replica) for High Availability
   a. Run the AuthMgr 7.1SP4 installable file.
      i. Select Replica instance for the installation type in setup wizard
      ii. When prompted, provide a path to the .pkg file generated in step 6 above
   b. After installation, follow the steps in Chapter 4 of the Installation and Configuration Guide to connect the primary and replica. Start the Security Operations Console on the replica (the only available Authentication Manager service that will be available) and trigger the connection function. It may run a long time.
   c. It is necessary to explicitly create a Radius server on the replica.
      i. Select Deployment Configuration → RADIUS → Configure Server.
      ii. Enter shared secret and administrator credentials - everything else happens automatically.

8. Confirm the replication link between primary and secondary nodes
   a. On Security Operations console, navigate to Deployment Configuration → Instances → Manage Existing.
   b. Click Check Replication Status link at the bottom of the page.
   c. The resulting Replication Status Report page provides direct or linked help for resolving any necessary actions.

9. Set up the tokens
   Note This step can be performed now or deferred until the remainder of the SecurID infrastructure is configured.
Solution Implementation

a. Import Token Records, supplied on compact disks (CDs) from RSA along with license files and the actual tokens, into the primary AM server.
   i. On Security console, navigate to Authentication → SecurID Tokens → Import Tokens Job → Add New
   ii. Follow steps provided in “RSA SecurID Token Records Getting Started Guide” on the token records CD.

b. To assign tokens to users, follow steps in the “Deploying Tokens to Users” section in Chapter 3 of the Administrator’s Guide.
   ii. Click the Unassigned tab
   iii. Select a token to assign.
   iv. Ensure the Assign to Users... is selected in the token list.
   v. Click Go.

Install and configure Citrix NetScaler VPX

This section contains steps for basic configuration of a high-availability NetScaler virtual appliance (VPX) installation on VMware vCenter as part of SecurID implementation.

After initial setup is completed, the following outline compliments detailed steps found in Citrix support document CTX131908, “How to Configure Access to Citrix Receiver Storefront 1.0 through AGEE.”

Important notes

- The NetScaler and Storefront versions cited in the document are earlier than those cited for this guide; however, the fundamental information remains viable. The fundamental goal is to provide a configuration foundation for SecurID service, upon which deployment-specific optimizations can be made.
- The steps below augment the document's standalone setup with high-availability configuration.
- NetScaler and Storefront configuration overlap to some degree and setup will be easier with careful planning of naming conventions, IP allocation, and certificate setup.

Before you begin NetScaler setup

- Be sure to record all information used, such as IP assignments, IDs and passwords, DNS aliases, etc. in tables provided in Appendix.
- Make sure Prerequisites in Chapter 3 are satisfied, with install media, SSL certificates, and networking information available.
- Configuration steps presented in this section apply to both the downloadable NetScaler virtual appliance (VPX) and hardware-based appliances.
Solution Implementation

- Authentication and session policy configuration involves a long series of nested dialogs. It is recommended that the installer print CTX131908 for use as a checklist. Record actual deployment information and notes in white space adjacent to dialogs and insure it matches corresponding items in Appendix.

References

- Citrix eDocs online documentation, linked from http://support.citrix.com. Locate and expand the NetScaler topic in the top-level contents pane. Full configuration and reference guides are found under Reference Material.
- Citrix support document CTX131908 - How to Configure Access to Citrix Receiver Storefront 1.0 through Access Gateway Enterprise Edition
- Citrix support document CTX109260 - How to Generate and Install a Public SSL Certificate on a NetScaler Appliance
- Citrix support document CTX122942 - How to Activate various Features and Modes of a NetScaler Appliance

Steps

1. Import the OVF template file onto the target VMware ESXi host to create the NetScaler virtual appliance
   a. Log into vCenter with administrator privilege
   b. Select File ➔ Import OVF Template... to open the Deploy OVF Template wizard
   c. The wizard is straightforward to VMware users. Complete the wizard to bring the NetScaler VPX online.
      For more information, refer to Citrix eDocs linked from the http://support.citrix.com support page (NetScaler ➔ NetScaler 10 ➔ Getting Started with Citrix NetScaler VPX ➔ Installing NetScaler Virtual Appliances on Vmware ESX)
2. Complete basic NetScaler configuration
   a. The VPX comes online as a BSD Unix guest. From vSphere, open a console to the VM and log in with default credentials (ID: nsroot / Password: nsroot).
   b. Start the initial configuration dialog by entering config ns
      i. At prompts, enter the appliance management IP (NSIP) and subnet mask.
      ii. Do not enter VLAN info under Advanced Network Configuration.
      iii. Save the configuration and exit.
   c. Browse to the NetScaler FQDN, which resolves to NSIP address entered in the preceding step to open the NetScaler GUI.
      i. The intuitive network setup wizard appears.
(1) A Mapped IP (MIP) address is required for setup. This address was allocated and recorded in Appendix with other required solution IPs in the prerequisite work prior to installation.

(2) After completing basic configuration, click link to set time zone.

ii. Configure DNS by navigating to DNS→Name Servers.

d. Licensing

i. Navigate to Configuration → System → Licenses GUI to add a .lic file. Reboot to enable.

ii. Licensed features must be explicitly enabled.

(1) Use Configure basic features link on Configuration → System → Settings page to activate features enabled by licensing.

(2) For activation via Command Line Interface (CLI), refer to Citrix support document CTX122942 - How to Activate various Features and Modes of a NetScaler Appliance.

3. Set up a NetScaler Access Gateway Enterprise Edition (AGEE) virtual server to provide external-network access to XenDesktop with SecurID (primary) and Active Directory (secondary) authentication.

a. Verify allocation of IP and DNS FQDN for the virtual server, previously recorded in Table A.

i. These are dedicated to the AGEE virtual server, separate from hostname FQDN, management IP (NSIP), and Mapped IP (MIP) of the appliance

ii. Ensure that nslookup can resolve IP to FQDN

iii. Confirm availability of an SSL certificate matching the virtual server FQDN

b. On NetScaler GUI console, navigate to Configuration → Access Gateway →Virtual Servers

c. Click Add...

d. On Certificates tab (default tab on opening), enter:

i. Name: Virtual server FQDN, recorded in Appendix

ii. IP Address: Virtual server IP (VIP address, recorded in Appendix

iii. Use default values for other fields.

iv. Install and bind the SSL certificate for this virtual server

(1) Certificate request should have been generated and ordered from Certificate Authority per Citrix support article CTX109260 as prerequisite work.

(2) CTX109260 also explains the simple installation process.

(3) After installation, the certificate appears in the “Available” list in left pane. Select the certificate and click Add button to move the certificate to “Configured” pane on right.
v. Authentication and session policy setup.

The referenced article, Citrix white paper CTX131908 is for NetScaler 9.3 and Storefront 1.0, but policies will work for NetScaler 10 with AGEE 9.2 and Storefront 1.2. Watch for updates for current versions.

Note

- The article also contains some steps for configuring Storefront. These steps overlap with the Storefront configuration section below.
- In Session policy setup, a URL to the VIP of the Storefront external-access load balancer (set up below) is entered in the Published Applications tab of the session profile. If post-configuration testing fails, replace the FQDN in the URL with IP address. If test then succeeds, check for name resolution or certificate issues.

vi. After initial AGEE setup, duplicate the primary and secondary policies that enable authentication against the primary RADIUS server (with lower priority) for the replica RADIUS server.

1. Enables authentication against the replica Authentication Manager node if primary becomes unreachable
2. Necessary because Authentication Manager does not respond to requests sent to a failed RADIUS server.

e. Add a Secure Ticket Authority (STA) for XenDesktop connectivity.

i. Navigate to Configuration → Access Gateway → Global Settings and click Bind/Unbind STA Servers to be used by the Secure Ticket Authority link under STA Servers.

ii. Click Add… in the popup dialog.

1. Enter the URL (using https:) of all the XenDesktop controllers in the environment (these provide the STA function) and click Create.
2. Click Close when done with additions.

Note The wizard appends "/scripts/ctxsta.dll" to the URL entered. This is NOT a physical path! Citrix XML services resolves the string appropriately. Besides, the added host displays the status only after the dialog is closed and re-opened.

4. Set up a load balancer to provide HA access to CloudGateway Storefront hosts

a. Set up Net Profiles to differentiate between external and internal access to XenDesktop

i. Browse to Configuration → Network → Net Profiles and click Add…

1. Enter a name to indicate use (External) and the Mapped IP (MIP) allocated for the purpose in Appendix table (IP set may also be used, requires allocation of more addresses)
2. Click OK
ii. Repeat for the Internal profile

iii. Close

b. Set up the Service Groups, one for external access and one for internal, to contain Storefront servers (which will be configured in next section)

i. Browse to Configuration → Load Balancing → Service Groups and click Add…

   (1) Enter a Service Group Name that identifies external access intent

   (2) On the Members tab:

      (a) In Specify Members field, leave IP Based default radio button on

      (b) Enter the management IP of primary Storefront node that is allocated for the task.

      (c) For Port, enter 443 (assuming SSL is used)

      (d) Leave default weight of "1" in place

      (e) For Server ID, leave None in place or enter a sequence number

      (f) Leave Hash ID field empty and Enable Member checkbox on

      (g) Click Add to enter the information in Configured Members pane

      (h) Repeat for the second and any subsequent Storefront hosts

   (3) On Monitors tab, select and add one or more monitors (such as https) which provide “up” or “down” status

   (4) Leave all other fields/tabs with default values

   (5) Click OK to create the service group

   (6) Repeat the preceding steps to create a service group for internal access - the Storefront server information is exactly the same.

c. Set up Load Balancer virtual server for external access to XenDesktop through Storefront

i. Install the SSL certificate for this virtual server using steps shown for the AGEE virtual server above.

ii. Browse to Configuration → Load Balancing → Virtual Servers and click Add…

   (1) Enter a Name that reflects use for external access and the IP address recorded in Appendix

   (2) Click Service Groups tab and select the external service group created in preceding steps
Solution Implementation

(3) Click **Methods and Persistence** tab
   (a) For LB Method, select **Least Connection**.
   (b) For Persistence, select **SOURCEIP** and ensure netmask is correct.
   (c) For Backup Persistence, select **NONE**.

(4) Click **Profiles** tab and select the external Net Profile created above from the dropdown list.

(5) On the **SSL Settings** tab, select the appropriate certificate in the **Available** tab and click **Add**.

(6) Click **OK** to create the virtual server.

(7) Repeat the preceding steps to create the internal-access load balancer virtual server.

5. Add the second NetScaler for high availability.
   
   a. Reference: **Citrix eDocs → NetScaler → NetScaler 10 → System → High Availability**
   
   b. Repeat steps 1-3 above to bring another NetScaler VPX online
   
   c. HA config is simple: Navigate to **Configuration → System → High Availability** and run the intuitive **Add...** dialog. All settings, IPs, etc. are replicated to the secondary appliance.

Install and configure Citrix Storefront

This section contains steps for a high availability Storefront deployment as the final component in the SecurID overlay for XenDesktop. The outline below compliments detailed steps found in the Citrix white paper *Citrix CloudGateway Express 2.0 Proof of Concept Implementation Guide*.

Important notes

- Citrix Storefront is synonymous with Citrix CloudGateway Express.
- As with the NetScaler setup, the fundamental goal is to provide a configuration foundation for SecurID service, upon which deployment-specific optimizations can be made.
- Repeat a caveat from the NetScaler setup section: NetScaler and Storefront configuration overlap to some degree and will be easier with careful planning of naming conventions, IP allocation, and certificate setup.

Before you begin Storefront setup

- Be sure to record all information used, such as IP assignments, IDs and passwords, DNS aliases, etc. in **Appendix**.
- Make sure Prerequisites above are satisfied, with install media, SSL certificates, and networking information available.
- Storefront installation and setup involves a long series of nested dialogs. It is recommended that the installer print the *Citrix CloudGateway Express 2.0 Proof of Concept Implementation Guide* for use as a checklist. Record actual
deployment information and notes in white space adjacent to dialogs and insure it matches corresponding items in Appendix.

References

- Citrix eDocs online documentation, linked from http://support.citrix.com. Storefront is found under the CloudGateway topic in the top-level contents pane.
- Citrix CloudGateway Express 2.0 Proof of Concept Implementation Guide - Citrix white paper

Steps

1. Install the primary Storefront instance as described in Section 1 of the white paper.
   a. SQL Database setup: A standalone database is required for a High Availability deployment.
      Note: This step assumes user familiarity with SQL Server, especially if a least-permissions approach to connectivity is desired.
      i. Follow setup steps in white paper to incorporate necessary database customizations.
      ii. Citrix eDocs instructions are online here: Citrix eDocs – CloudGateway → StoreFront → StoreFront 1.2 → Install and Set Up → Configuring StoreFront → To Deploy a multiple server group
   b. Install Storefront SSL certificate recorded in Appendix as described in the white paper.

2. Complete initial configuration per Section 2 of the white paper.
   a. Create Server Group
      i. Click Deploy Multiple Server Group, and enter the FQDN of the internal load balancer virtual server created during NetScaler setup. It is imperative that this step be completed with proper FQDN in place as it cannot be altered later.
         (1) The field is pre-populated with a URL pointing to the local host. This URL will work as long as this instance is available, but eliminates HA functionality - and, reiterating, this value cannot be edited later.
         (2) For SQL values, enter FQDN of SQL host and Database name described in Step 1-a above and click Test Connection to confirm connectivity.
      ii. Click Create.
   b. Create Store.
      i. On Store Name screen, enter an appropriate name that helps users identify the target XenDesktop environment; this name appears inside the Receiver client. Click Next.
      ii. On Add Delivery Controllers dialog, enter the XenDesktop controller FQDNs. Click Next.
Note Subsidiary screens used in the add process are intuitive and not described here.

iii. On Remote Access screen, use default No VPN Tunnel. Click Add...  
1. On Add Gateway Server screen, enter the following information and click Next.  
   a. Display name for Gateway Server  
   b. Gateway URL - use FQDN of NetScaler Access Gateway virtual server)  
   c. Deployment mode: Appliance  
   d. Set Server as Access Gateway Enterprise Edition: [on]  
   e. Subnet IP address: use Mapped IP (MIP) created for purpose in NetScaler setup  
   f. Logon type: Domain and Security Token  
2. On Enable Silent Authentication screen, enter FQDN of Access Gateway virtual server. Citrix adds the rest of URL. Click Next.  
3. On Secure Ticket Authority (STA) screen, click Add...  
   a. Enter URL of XenDesktop host, which serves as STA.  
   b. Note that Citrix appends "/scripts/ctxsta.dll" to the URL entered. This is NOT a physical path in XenDesktop 5.x, Citrix XML services resolves the string appropriately.  
   c. Click Create.  

iv. Setup is Complete screen appears. Click Finish.  
v. Citrix Storefront screen is presented, with large buttons to:  
1. View or Change Stores  
2. Create Another Store  

3. Enable pass-through authentication per instructions at the end of Section 2 of the white paper.  

3. Set up secondary Storefront host per Section 3 of the white paper.  

a. Install Storefront on a new host  
b. When Storefront starts, click join existing server group  
   Join server group window opens with fields for Authorizing Server and Authorization Code. No action is taken now; proceed to the next step.  
c. On the primary server, select Server Group in the left pane.  
   i. Click Add Server in right pane.  
   ii. Authorize new server window opens and shows authorizing server and authorization code. Leave this dialog open.
d. On the secondary host, enter the server and authorization code from the preceding step in Join Server Group fields and click Join.

e. Both servers should report a successful join in the open dialogs. Click OK on both to acknowledge.

f. On primary host, click Propagate Changes in the right pane.

4. After finishing the propagation step, configuration of Storefront and SecurID deployment are complete.

Backup and recovery implementation

**RSA Authentication Manager**

RSA recommends use of Authentication Manager built-in functions for its internal database backup. Refer to the Authentication Manager Administrator’s Guide for more information. Backup of the relatively small internal store is not expected to require additional hardware or compute resource.

**Citrix NetScaler VPX, Citrix Storefront**

Backup and recovery for these components falls under guidelines for the overall VSPEX XenDesktop solution, described in the appropriate infrastructure document.
Solution Implementation
This chapter presents the following topics:

Baseline hardware validation .............................................................. 40
RSA SecurID functional validation ....................................................... 40
Functional validation methodology.................................................... 44
Solution Validation

Baseline hardware validation

Hardware validation is beyond the scope of this document. Refer to the VSPEX XenDesktop virtual infrastructure documents for more information.

RSA SecurID functional validation

Broadly speaking, the SecurID deployment methodology used in this overlay fits the “three-legged stool” metaphor. All three major components – RSA Authentication Manager, Citrix NetScaler, and Citrix Storefront – must be properly configured to enable a successful SecurID authentication and subsequent login to a VSPEX XenDesktop virtual desktop. If any of the components is misconfigured, login will fail.

With that said, it is possible to successfully authenticate with Authentication Manager but still fail to be connected to the target virtual desktop due to NetScaler Access Gateway or Storefront misconfiguration.

Authentication Manager provides monitoring tools for direct verification of successful SecurID authentication. Monitor activation steps are provided below.

Troubleshooting the post-authentication NetScaler → Storefront → XenDesktop connection is more complex due to the high number of handshakes among NetScaler, Storefront, and XenDesktop. Testing shows the two most likely causes of failure to connect are:

- Name resolution errors: ensure that DNS can resolve FQDNs used in configuration of each component.
The following steps are used for a browser-based login to a virtual desktop through NetScaler’s Access Gateway with SecurID and Active Directory authentication:

1. Browse to the external access path configured in Step 3 under “Install and configure Citrix NetScaler virtual appliance” above; for example, http://ExternalAccess.MyDomain.com

2. On the default login dialog shown in Figure 2, and enter:
   a. User name: Unqualified AD userid (MyUserID instead of domain\MyUserId)
   b. Password 1: AD password
   c. Password 2: SecurID passphrase

   ![Default Access Gateway login dialog]

   Figure 2. Default Access Gateway login dialog

3. Successful validation triggers loading of the browser-based Citrix Receiver client.
   a. Entry of incorrect AD password or SecurID passphrase results in an immediate error message displayed on the dialog.
   b. See “Functional validation methodology” below for steps to activate the SecurID activity monitor.
4. The Citrix Receiver client is loading, shown in Figure 3. This can be slow on initial access or after component reboots.

Figure 3. Browser-based Citrix Receiver client – automatic login to virtual desktop in progress

5. Login to the desktop is carried out with no further user interaction.

Note A certificate error can manifest here with a variety of http or other errors appearing and the logon process aborted.
The following steps are used for a browser-based log in through NetScaler’s local-access load balancer with Active Directory authentication:

1. Browse to the internal access path configured in step 4.c under “Install and configure Citrix NetScaler virtual appliance” above; for example, http://InternalAccess.MyDomain.com

2. The Citrix Receiver client loads with Active Directory authentication challenge, shown in Figure 4. Enter credentials and click Log On.

3. The user is logged into the desktop.

   **Note**  As with external-access login, certificate errors can manifest here with a variety of http or other errors appearing and the logon process aborted.
Solution Validation

Functional validation methodology

Proper operation of the following functions must be tested:

- Authentication: For external access, improper credentials, whether userid, AD password, or SecurID passphrase, generates a generic error message that does not identify which value is incorrect. For internal access, only Active Directory credentials are required and similarly validated.

- Single sign-on: After authentication, user login takes place with no additional challenge at the desktop.

Key metrics

Beyond proper operation at the VSPEX virtual infrastructure increments of up to 250 desktops (using EMC VNXe storage) or up to 2000 desktops (using EMC VNX storage), no metrics were generated for the overlay. SecurID has no effect on XenDesktop performance after authentication is complete.

Define the test scenarios

Authentication Manager

Authentication success:

- Presentation of the authentication dialog prompting for SecurID name and passcode and subsequent successful authentication is the de facto success criterion.

- If more information is desired, the following steps can be taken.
  a. On Authentication Manager’s Security Console, open Reporting → Realtime Activity Monitors → Authentication Activity Monitor. If desired, enter the user name to be verified in the Search field.
  b. Click Start Monitor
  c. Log into a desktop through the Access Gateway client, shown in Figure 4
  d. In the monitor window, verify that SecurID credentials are validated
  e. Close the monitor

Basic High Availability function can be tested in the following procedures:

a. Using VMware vSphere, edit the settings for the primary Authentication Manager node to disconnect the guests’ virtual NIC, or shut down the guest.

b. Verify successful SecurID authentication.

c. Reconnect the primary node virtual NIC.

d. Repeat the preceding with secondary node virtual NIC disconnect or shutdown.

NetScaler

- Normal operation is verified by ability to successfully log in to desktops.

- High Availability (for active-passive configuration):
  a. Disconnect the primary NetScaler from the network or shut it down
Solution Validation

b. Log in to the secondary node and navigate to **System → High Availability**, where primary/secondary status is displayed.

   **Note**  Login to a non-primary node results in a dialog warning that configuration changes will not be propagated.

c. Verify that user logins via internal and external paths work as expected.

d. Reconnect or restart the primary node.

e. Repeat the test for the secondary node. (Note: Once failover has occurred, the “new” primary node will remain primary when the “failed” host is brought back online unless a forced failover returns the two hosts to the original settings.)

**Storefront**

- Normal operation is verified by ability to successfully log in to desktops.

- High Availability:

  a. Using VMware vSphere, edit the settings for the primary Storefront node to disconnect the guests’ virtual NIC, or shut down the guest.

  b. Verify successful login to user desktop through internal and external path.

  c. Reconnect the primary node virtual NIC or restart the guest.

  d. Repeat the preceding with secondary node virtual NIC disconnect.
Chapter 6  Reference Documentation

This chapter presents the following topics:

White papers .............................................................................................................. 48
Product documentation .......................................................................................... 48
Other documentation ............................................................................................. 48
Reference Documentation

White papers

For additional information, see the white paper listed below.

- Citrix CloudGateway Express 2.0 Proof of Concept - Implementation Guide

Product documentation

For additional information, see the product documentation listed below.

- Securing VSPEX Citrix XenDesktop 5.6 End-User Computing Solutions with RSA, VMware vSphere 5.1 for up to 2000 Virtual Desktops - Design Guide
- EMC VSPEX End-User Computing: Citrix XenDesktop 5.6 and VMware vSphere 5.1 for up to 250 Virtual Desktops Enabled by EMC VNXe, and EMC Next Generation Backup
- EMC VSPEX End-User Computing: Citrix XenDesktop 5.6 and VMware vSphere 5.1 for up to 2000 Virtual Desktops Enabled by EMC VNXe, and EMC Next Generation Backup

Other documentation

For additional information, see the documents listed below.

- RSA Authentication Manager 7.1 Installation and Configuration Guide
- RSA Authentication Manager 7.1 Administrator’s Guide
- RSA Authentication Manager 7.1 Performance and Scalability Guide
- CitrixCTX131908: How to Configure Access to Citrix Receiver Storefront 1.0 through Access Gateway Enterprise Edition
Appendix A  Configuration Information

This appendix presents the following topics:

Table of required configuration information ......................................................... 50
Table of required configuration information

### Table 2. Required configuration information for RSA Authentication Manager

<table>
<thead>
<tr>
<th></th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter (ESXi) host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install media location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>License and token record file location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local admin ID/password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Secret</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 3. Required configuration information for Citrix NetScaler VPX

<table>
<thead>
<tr>
<th></th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management IP (NSIP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Setup Mapped IP (MIP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter (ESXi) host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OVF file download location</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4. Required configuration information for Access Gateway Virtual Server

<table>
<thead>
<tr>
<th>Virtual Server Name (FQDN)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual server IP (VIP)</td>
<td></td>
</tr>
<tr>
<td>Virtual Server Certificate</td>
<td></td>
</tr>
</tbody>
</table>

### Table 5. Required configuration information for NetScaler Load Balancers

<table>
<thead>
<tr>
<th>Name / Mapped IP</th>
<th>External</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net Profile Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Group Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Server name / IP</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Virtual Server Certificate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 6. Required configuration information for Storefront

<table>
<thead>
<tr>
<th>Hostname (FQDN)</th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter (ESXi) host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install media location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL server / database</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>Server Group URL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Store Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XenDesktop Hosts</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>