

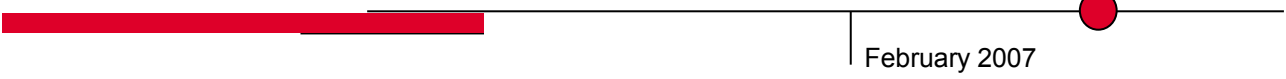
Novell Satellite Site Appliance

Technical Outline

prepared for

Connecting for Health

www.novell.com



February 2007



Novell[®]

Disclaimer Novell, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Trademarks Novell is a registered trademark of Novell, Inc. in the United States and other countries.

* All third-party trademarks are property of their respective owner.

Copyright 2007 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of Novell, Inc.

Novell, Inc.

404 Wyman

Suite 500

Waltham

Massachusetts 02451

USA

Novell UK Ltd

One Arlington Square

Downshire Way

Bracknell

Berkshire

RG12 1WA

UK

Prepared By David Shepherd

Novell Satellite Site Appliance—Technical Outline

February 2007

Statement of Work: SOW #

Connecting for Health Number: Client #

Consultants: Consultant/s

Revision History

Version	Date	Editor	Revisions
0.5	2 nd Feb	David Shepherd	First Draft

Reviewer Record

Version	Date	Reviewers Name	Reviewers Role (Peer/ Team Leader / Project Manager)

Final Approval

Version	Date	Reviewers Name	Reviewers Role (Peer/ Team Leader / Project Manager)

Contents

Executive Summary	1
Technical Outline	2
Satellite Site Appliance Hardware Specification.....	4
Satellite Site Appliance Modules.....	4
Core Module Description.....	4
Optional Modules.....	5
Provisioning Users and Applications to the SSA.....	6
Provisioning of Users.....	6
Provisioning of Applications.....	7
Solution Advantages.....	8
Standard Small Site Solution.....	8
Utilisation of Existing Software Licenses.....	8
The Use of Open Source Software.....	8
Centralisation of Support.....	8
Efficient Use of Wide Area Network Bandwidth.....	8

Tables

Figures

Executive Summary

The aim of this document is to outline the technologies that form part of the Novell Satellite Site Appliance. This device is ideal for any large organisation that have a large number of small sites that may not have high bandwidth or secure connectivity back to a central location. This makes management of small remote sites quite difficult when the remote location has limited local IT Support and whilst each site is only serving small numbers of users the importance of a reliable and well managed infrastructure cannot be underestimated.

Within the context of the NHS this scenario matches Doctors Surgeries and other dispersed locations with small numbers of staff (not necessarily skilled in any form of IT Support Function) at locations where there may only be relatively weak connectivity (at least 2MB ADSL is assumed) back to the central location.

It is also important to understand that this is not an out of the box Novell Product. It does have some Novell Consulting components that deal with some of the provisioning requirements discussed later in the document.

Please note that the discussion here involves a number of Open Source technologies. How the combined solution will be supported in an NHS environment is not discussed here and this would need to be part of a separate process.

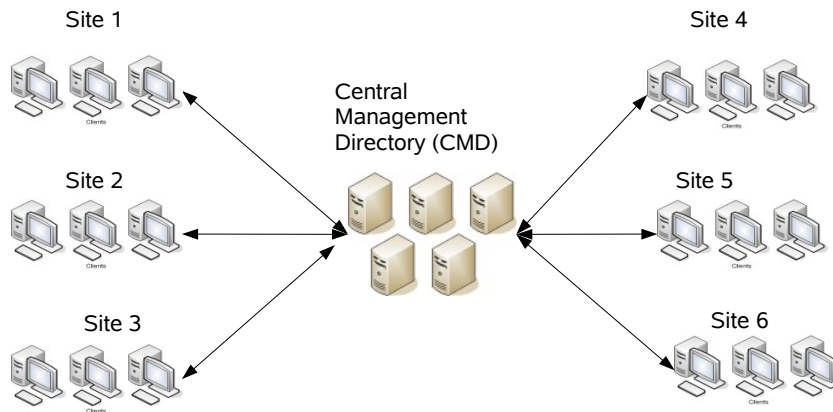
Technical Outline

The aim of this section is to provide an overall outline of the solution and its components. The primary focus is to deliver a local site server infrastructure in the form of an appliance based solution. This appliance will be modular in nature and deliver a number of services to the local site. It is envisaged that a number of these appliances can be delivered and managed from a central location. This central location will have both IT Support Personnel and the communication infrastructure to allow for management and provisioning of the solution. The appliance build will have a standard core and a number of modules could be optionally added to provide extra functionality. These modules could be added either at the time of deployment or later in the devices life cycle.

Minimal day to day management will be required from the local site perspective with centrally controlled processes in place for the following items:

- Provisioning of user accounts
- Provisioning of applications
- Management of the local client devices
- Server management and monitoring
- Backup of local site data
- Management of local site Printers
- Remote administration of the environment.
- Virus Protection of the Workstation and Server.

The solution is based around a Central Management Directory (CMD). The CMD could be an existing instance of eDirectory or a specialised Management Directory. This eDirectory can easily sit next to an existing Novell Infrastructure or a Microsoft Active Directory. The functionality discussed here can be delivered as an integrated component of the **NHS Beacons** project that is currently under way with Novell. The CMD holds objects that represent each of the Site Appliance Servers, their users and applications. Users and Applications are provisioned by the assignment of directory based objects to Satellite Site Appliance Server (SSA) Objects held in the Central Directory. One CMD could easily manage 100 plus Satellite Servers but all administration is controlled and managed from the CMD.



The links from the CMD to the sites in the diagram do not require large amounts of bandwidth. The connection required for user and application provisioning is described as a 'point in time' connection, whilst each site has its own simplified and easily managed directory there is no requirement for that directory to contact the CMD on an ongoing basis. The user and application provisioning process attempts to contact the sites with the information that needs to be provisioned. It only executes this process when there is a provisioning request. If the link or the site is down then this process backs off and is retried later. If any connection errors occur when transferring data to the site then the process uses a check point based restart. This means that the data stream is backed up in accordance with the size of the checkpoint and the process is retried with no data loss. Local functionality and services are in no way impaired if the connection to the centre is down.

The CMD staff will have the ability to contact and manage the site in a number of ways.

1. The normal application and user provisioning process.
2. Via a secure VNC Connection to the server device to use any graphical tools.
3. Via a secure SSH Session to allow management via a character based interface. This will allow a number of management tasks to be undertaken via the command line console. These will include change of a users password, add of a user (outside of the normal provisioning process), and various other monitoring tools and directory repair tools.
4. Via the ZENworks remote client management tools..

Satellite Site Appliance Hardware Specification

This section describes the proposed hardware specification of a site based server. This specification should serve to provide a good estimate of the requirements based on the likely numbers of users at most Doctors Surgeries.

- CPU Requirement – Intel Pentium 4 (3GHz) or greater. Dual Core would be recommended depending on the modules deployed.
- Memory Required. - 2GB of RAM (4GB of RAM if more of the modules are deployed).
- Disk Space - At least 150GB of disk (SATA/SCSI) deployed as a Raid 1 Mirrored Pair. They should also be hot swappable.

Depending on the Service Level agreement required, it would be advisable to have an off-line spare already deployed on site. In case of hardware failure including one disk it would be possible to remove one disk of the pair in the failed device and replace this in the new server, and then bring the server on-line.

If a new server were required for the site then an empty appliance could be deployed to the site and, users, applications, and policies could be re-deployed from the centre.

Satellite Site Appliance Modules

As has been discussed earlier, the site appliance will be delivered in a modular form with one core Module and any number of additional modules as required by the staff at the local site. These modules are build components that could be combined so that a standard DVD could deliver the solution with as little as five pieces of information required by the build process.

- IP Address – Address of the site device.
- IP Subnet Mask
- IP Gateway
- Address of DNS Server plus backup address.
- Name of the Server.

Core Module Description

This core module is the base build of the site based server appliance. This is able to be deployed on one of two scenarios.

1. There is no other SSA deployed on the site so a Primary Image is used.
2. There is an existing SSA deployed. In this case a Secondary Image is used and needs the location of the Primary Device. Certain directory information is synchronised between the two systems to provide resilience in case of failure of either device. This would also allow for the scaling of the devices in sites that have perhaps more than 100 local users.

The Core Module itself is responsible for the following functionality:

1. Base hardened OS Build – Novell OES Linux Server SP2 (SLES 9 SP3 is the base code). Later this year OES Version 2 is launched and the base OS would become SLES10 SP1.
2. Deployment of a local DNS Caching server. This would not hold any local zone information but would cache local site requests so that subsequent DNS resolution requests would be resolved locally. A DHCP Server could also be deployed as part of the base build.
3. Configuration and deployment of Novell App Armour. This is an application level Firewall that mandates each applications abilities to communicate to other modules and any file-system changes that they make as part of their normal operation.
4. Deployment of a simplified and secure local e-Directory instance for the site. This would be a common layout for every SSA Server deployed and would hold users, applications, and policies for the location.
5. Deployment of a shareable portion of the file system of the device. This would allow the following areas of the system to be configured. A system area that would hold application code, a users home directory area that would hold individual users data and a shareable area that would allow data to be exchanged between users. These areas would be backed up over night to the central location in accordance to a user definable schedule. This backup process would take place through an SSH encrypted tunnel. This tunnel could also be wrapped within the site-site VPN.
6. Deployment of ZENworks for the local site. This includes application delivery, policy lock down of Windows Devices and remote control of the client systems. Application delivery includes the distribution of code from the central location and the installation of that code from the local server to the workstation device. This functionality will be enforced by the users rights and access privilege's within the local server. This would include a process to deploy agent code on the clients first access of the system.
7. Deployment of a configured Anti-Virus solution that would deploy agent code to client devices on their first connection to the appliance.
8. Deployment of a Network Printing Solution.
9. Deployment of a solution that would enable data to be backed up from the device over the wire to the CMD. This would be a scheduled process and take place over night.

Optional Modules

- VPN / Internet Access. Squid is used to provide an Internet Proxy based around the users local site directory credential. VPN could be provided by a number of Linux based applications that provide a site to site VPN. One open source product that could be used to provide this module is OpenVPN.
- Wireless Access Point. -1. The deployment of this module plus a PCI based Wireless access card will enable secure wireless access for the site based on WPA. Again this will be managed against the users identity in the local directory. Again at least one open source solution exists to manage this.

HOSTAPD is an open source project that has already been added as a component of the 2.6 Linux Kernel..

- Wireless Access Point – 2. This may be the preferred option where a Radius Server is added to the site appliance and the Access Point is delivered as a separate device. Wireless Access points are common hardware devices that can provide a number of services to the remote site. The use of WPA and Radius ensures wireless security and in case of hardware failure the external access point would be more easily replaced than option 1.
- Client Device Backup. This allows for any data held on the client device to be transparently backed up to either the local site appliance device or to the Centralised Management Directory. This process is transparent to the user and allows a simpler replacement of the client device in case of theft or hardware issues.
- Smart Card Support. This again could be provisioned from a central directory and the details pushed out to the site appliance. An important aspect of this is that if users came from the site into the main trust location they would be able to use the same Smart Card to gain access to systems within that location.

This list is by no means exhaustive and could easily be extended at a future date to add further functionality.

Provisioning Users and Applications to the SSA.

The issue that the solution is attempting to solve is that how best can you manage a small site from a central location whilst requiring minimal local support of the overall process. Key to this process is the provisioning of users and applications to the device over time.

It is envisaged that users at the local site would only have very elementary management capabilities to their local device.

This would include the ability to change a users password and the ability to enable or disable an existing user. It is important to understand the relationship of the CMD to the local Site appliance. The site appliance is a separate directory to the Central Management Directory and does not need to synchronise with it in the traditional sense. It is based on a point in time connection, when a process from the CMD calls out to the site server. If the Site Server is unavailable then the request is queued and retried at a later date. This process requires a relatively small amount of bandwidth and only happens when a user or application is assigned to a particular Satellite Site Appliance.

Provisioning of Users.

Within the Central Management Directory the user account is created and a password assigned.

1. This user is then assigned to a particular site SSA Server. These servers are represented by objects in the directory and conceptually the process is the same as assigning users to a group.
2. This triggers a directory event that the provisioning process is looking for and creates a provisioning request file. For a user and password this file can be as small as 150 bytes.

3. This file is taken via a component of ZENworks called ZEN for Servers. This allows the delivery of the file in a secure manner to the site appliance. If the site appliance is not available then the copy is backed off and retried until successful.
4. Once the file has been delivered to the SSA Sever the file is timestamped in accordance with the local devices clock. This file is then processed by a component called the un-bundler which is responsible for acting on the provisioning request and creating the user based on the information in the CMD.

Any subsequent Modification to the User are carried over in a similar manner to the previous paragraph.

Changes to the users password from the local site are also synchronised back to the CMD.

Within the basic user provisioning process there are a number of things to keep in mind.

- A user could be automatically assigned to a number of SSA Servers if required. This process would work in accordance with the description given at the start of this section.
- A user when de-assigned from the object in the Central Management Directory could be either removed from the SSA Server or disabled from authenticating depending on the policy required defined by the NHS.
- The provisioning process could be extended to include Smart Cards.

Provisioning of Applications.

The application provisioning is handled in two stages. The Application object is defined under the SSA Server object that resides in the CMD. The object is a schema extension that is also defined as a container.

- ZEN for Servers has the ability to move both application data and application object definitions between eDirectory instances. The advantage of ZEN for Servers is that you can bandwidth throttle the link and also use checkpoint restarts.. This allows both for the distribution of the code and the application object. The object allows the user to see the application as available for use on their client workstation.
- Application objects that are created in the CMD will also require the assignment of users that also exist within the SSA Server. This assignment is also handled centrally with the request being synchronised locally to the local eDirectory instance.

Solution Advantages

The solution as described would offer a number of advantages for Connecting for Health.

Standard Small Site Solution

The definition and deployment of a standard solution. All Doctors Surgeries within the NHS would have a similar functional requirement. The deployment and maintenance of each site becomes standard with only the users and themselves and perhaps the applications deployed being different. Having a standard hardware platform will also assist in maintenance and purchasing costs. From a client side the definition of a standard NHS Small Site client build could also be beneficial.

Utilisation of Existing Software Licenses.

The use of existing purchased software. Some of the components discussed here are Open Source in nature but others of the products fall within the software that has already been purchased by the NHS.

The Use of Open Source Software

Using a Linux base as described in the technical outline opens up the potential use of many different industrial strength open source projects.

Centralisation of Support

Centralisation of the Management of the Device. A number of these small site devices could be managed from a central location. This central location would provide the following services.

1. User Provisioning
2. Application Provisioning
3. Centralised Backup of Data
4. Management and Monitoring
5. Control of the application of patches to the SSA Server and preserving the stability of the build.

Having a set of standard practises that apply to a number of the Satellite Site Appliances will also provide efficiency benefits. The Central Management location would also be responsible for mandated the tested applications and the Client side configuration that would be required.

Efficient Use of Wide Area Network Bandwidth

The use of the WAN is kept to a minimum with this approach during the normal office hours.

<End of Document>

Novell.[®]

Proposed Deployment
