Centrify DirectControl-Enhanced PuTTY

Version 3.0.7

Published: August 2007

Abstract

PuTTY is a popular open-source tool that provides Telnet, SSH, rlogin and raw TCP client functionalities for Win32 and UNIX-based platforms. Centrify has enhanced this tool to provide Kerberos-based authentication to UNIX and Linux computers; so that it works seamlessly with DirectControl-managed systems.

This document describes how to install the Centrify-enhanced PuTTY tool and configure the different Kerberos options.

The Centrify's version of PuTTY is currently available on Windows platforms only.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Legal notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

© 2004-2007 Centrify Corporation. All rights reserved. *Portions of Centrify DirectControl are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.*

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify and DirectControl are trademarks of Centrify Corporation in the United States and/or other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

Abstract **1**

Legal notice **2**

Contents **3**

1 Overview **4**

1.1 PuTTY's Version 4

1.2 Conventions Used 4

2 Installing Centrify DirectControl-Enhanced PuTTY **5**

2.1 Supported Windows Platform 5

2.2 Centrify DirectControl and Centrify OpenSSH 5

2.3 Installation Procedure 5

3 Centrify PuTTY Configuration **7**

3.1 Configuring for Kerberos Authentication 7

4 Centrify PuTTY Group Policy Settings **12**

5 PuTTY related utilities **15**

5.1 Example 16

6 References **17**

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

1 Overview

PuTTY is a popular open-source client on Windows and UNIX-based systems that provides access to remote machines using well-known network protocols such as Telnet, SSH, rlogin and raw TCP. However, it does not support Kerberos authentication.

Centrify has enhanced the PuTTY tool so that user authentication can be accomplished using Kerberos before establishing a remote connection. Since the Centrify DirectControl Agent sets up a Kerberos environment on managed UNIX and Linux computers, this allows a seamless integration into DirectControl-managed systems. Thus, you gain the benefits of centralized authentication and password policy enforcement using a secure and well-established authentication infrastructure.

Centrify PuTTY also interoperates with the Centrify OpenSSH utility. The Centrify OpenSSH configuration (`sshd_config`) uses Kerberos authentication by default. It also handles different forms of user name for Unix login.

This document describes how to install Centrify-enhanced PuTTY and configure the Kerberos options for use by the SSH protocol. The current version of Centrify PuTTY is implemented on the Windows platform only.

1.1 PuTTY's Version

The Centrify's enhanced version is based on PuTTY version 0.60, released in April 2007.

1.2 Conventions Used

The following conventions are used in this document:

- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *`italicized`*, the `fixed-width` font is used to indicate variables. In addition, in command line reference information, square brackets ([ ]) indicate optional arguments.
- *Italics* are used for book titles and to emphasize specific words or terms.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- For simplicity, we will use Unix in this document to refer to all DirectControl supported versions of the UNIX and Linux operating systems unless otherwise noted.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

2 Installing Centrify DirectControl-Enhanced PuTTY

This section provides pre-installation information before as well as the installation procedure for the Centrify PuTTY software.

2.1 Supported Windows Platform

This version of Centrify PuTTY software supports the following Windows platforms.

- Windows 2000 Professional SP4
- Windows 2000 Server SP4
- Windows XP SP1, SP2
- Windows 2003 SP1, R2
- Vista (32-bit)

Since the support platforms may change in future, please contact Centrify Support for the most up-to-date list.

2.2 Centrify DirectControl and Centrify OpenSSH

You can use Centrify PuTTY to remotely access any UNIX and Linux machines. However, if the Centrify DirectControl Agent has been installed on the UNIX/Linux machine, users can securely access remote computers via the SSH protocol using Active Directory credentials. DirectControl can also deduce the Unix login name from the User Principal Name (UPN) in Active Directory, thus making it possible for a user to do secure Single Sign-on to all machines with a single Active Directory identity. Administrators have the added benefits of accelerated deployment since DirectControl already sets up a Kerberos environment on the target machines. As an example, there is no need for DNS-to-realm mapping because DirectControl already knows the relationship between the hosts and their Service Principal Names (SPNs).

This version of Centrify PuTTY (3.0.7) works with Centrify DirectControl version 3.0.5 and above. It interoperates with Centrify OpenSSH version 3.0.7 and above.

2.3 Installation Procedure

The Centrify PuTTY software is installed by executing the following steps.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

1. Double click on the `msi` file containing the PuTTY software to launch the Setup Wizard. If another version of the software already exists, you will be prompted to remove it before you can proceed. Otherwise, a Welcome page appears.

2. On the Welcome page, press **Next** to continue.

3. On the **Select Installation Folder** dialog,

    a. Choose the folder where the software should be installed by either selecting the default location (`c:\Program Files\Centrify\PuTTY`) or input the destination folder.

    b. Specify who can use the PuTTY utility on this computer.

    c. Press **Next**.

4. You will be asked to confirm the installation. Press **Next** to start the installation.

5. An **Installation Complete** screen should appear upon successful installation.

In addition to installing the PuTTY program (`putty.exe`), other PuTTY related utilities will also be installed. These utilities are:

- `pageant.exe`: an SSH authentication agent for PuTTY, PSCP and Plink
- `plink.exe`: a command-line interface to the PuTTY backend
- `pscp.exe`: an SCP client (command line secure file copy)
- `psftp.exe`: an SFTP client
- `puttygen.exe`: an RSA and DSA key generation utility
- `puttytel.exe`: a Telnet-only client

Please refer to the official PuTTY documentation for detailed information of these programs.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

3 Centrify PuTTY Configuration

Centrify enhances the open-source PuTTY tool by adding the capability to use the Kerberos authentication mechanism for remote access via the SSH (Secure Shell) network protocol. It adds an SSH Kerberos configuration page to the Windows interface. All other functionalities remain the same as in the official PuTTY software.

3.1 Configuring for Kerberos Authentication

When you invoke the Centrify PuTTY program after installation, the first screen is the same as the open-source PuTTY.

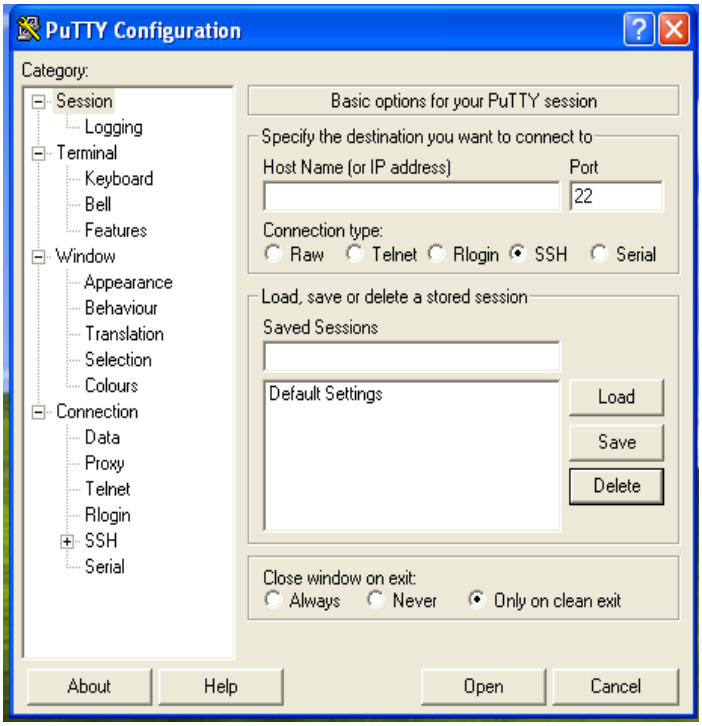

Figure 1 PuTTY Initial Page

When you expand **SSH** under the Connection tree, you will see a new node, **Kerberos**, as illustrated in the next figure.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

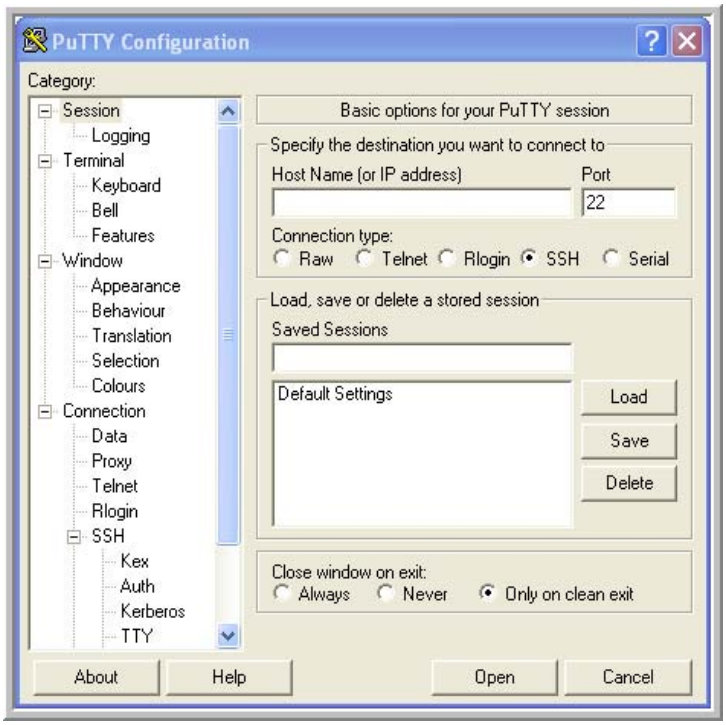

Figure 2 Expanded SSH Node

When you click on **Kerberos**, the Kerberos configuration page is displayed, as follows.

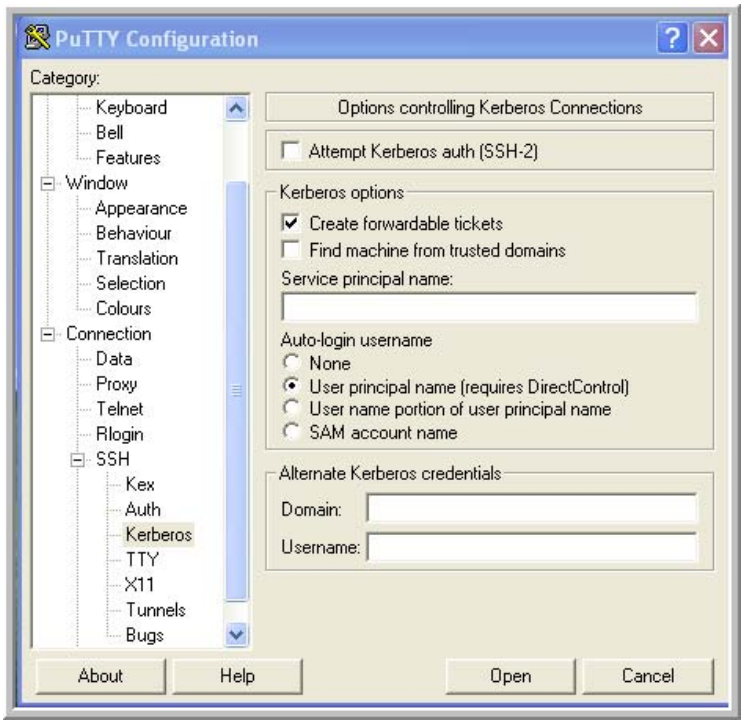

Figure 3 Kerberos Configuration Page

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

The following describes the different configuration options on this page. Please note that the settings affect SSH connection only.

The first option, **Attempt Kerberos Auth (SSH-2)** specifies whether the new SSH session will use Kerberos authentication or not. Note that only SSH-2 is supported. SSH-2 contains security improvements and feature enhancements over SSH-1. The default is unchecked, which means the PuTTY program will use the authentication mechanisms defined in the **Connection->SSH->Auth** page. If this option is checked, Centrify PuTTY will try to establish the connection using Kerberos first. If it fails, then the other authentication mechanisms defined for SSH will be used.

The next panel, K**erberos options**, contains the various options used to locate the target machine and define the Unix login name. It contains the following fields:

- **Create forwardable tickets** specifies whether the target server can use the same Kerberos credentials for authentication with other Kerberos-based services. The option is checked by default, thus allowing the user of this SSH session to silently login to other SSH servers without providing any password. Otherwise, the user will be prompted for password when connecting to another Kerberos-authenticated service.

- **Find machine from trusted domains** specifies whether Centrify PuTTY should look for the destination machine from the trusted domains if it cannot locate it in the currently login domain. This may happen, for example, if the target Linux/UNIX machine resides in an external domain. Note that this will require the PuTTY program to initiate an LDAP connection to the domain controller in the trusted domains using the login user's identity. Thus, the attempt will succeed only if the domain controller is accessible and the user has the appropriate READ access in Active Directory. The default for this option is off. If Centrify PuTTY cannot locate the target machine, the user will be prompted to provide another set of Kerberos credentials, as shown in Figure 4. You can control the LDAP connection setting by using the Centrify PuTTY Group Policy. Please refer to Section 4.

- **Service principal name** allows the user to explicitly specify the Service Principal Name (SPN) of the target machine. This is necessary if the target machine is in a different forest, and the PuTTY program cannot access the Kerberos Distribution Center (KDC) for the target machine - either because the **Find machine from trusted domains** is not checked or the firewall settings prevent making an LDAP connection to the domain controller in the trusted domains.

- **Auto-login username** provides several options to specify the Unix user account name for the SSH session. They are:

    - **None**: Centrify PuTTY will not automatically generate the Unix account name. Instead, the user will be prompted to type in the user name for Kerberos authentication. To avoid typing in the login name each time,

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

the user can define the default value in the **Auto-login username** field in the **Connection->Data** configuration page.

- **User principal name (requires DirectControl)**: This is checked by default. In this case Centrify PuTTY will use the login user's User Principal Name (UPN) as the Unix account name. For this to work, the DirectControl software needs to be installed on the target machine. There is no need for a `.k5login` file in the user's Unix home directory since DirectControl automatically maps the UPN in the Kerberos ticket to the Unix profile for the Active Directory username presented in the ticket.

- **User name portion of user principal name**: Centrify PuTTY will use the user name portion of the UPN as the Unix login name. For example, if the UPN is `jdoe@xyz.com`, `jdoe` will be used in this case.

- **SAM account name**, if selected, will cause Centrify PuTTY to look up the SAM account name in Active Directory and use it as the Unix account name. Note that this will initiate an LDAP connection to the currently logged-in domain controller. If the lookup fails for any reason, Centrify PuTTY will prompt the user to enter the Unix name.

The next panel, **Alternate Kerberos credentials**, allows the user to not use the current Kerberos credentials (the one used for logging into the Windows machine) for authentication, which is the default; and to specify a different set instead. To use this capability, the user would need to fill in the **Domain** and **Username** fields. When the connection is made, the following dialog will be displayed prompting for a password.

Figure 4 Password Prompt

The user can select the **Remember my password** checkbox so that the Windows credential manager will cache the password and not prompt for one again the next time the same remote machine is accessed. Hence the user can Single Sign-on remotely to

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Unix machines using his Active Directory user credentials. When entering the password, the user is given a number of tries before failing the Kerberos authentication and resorting to other SSH authentication mechanisms. The ability to use alternate Kerberos credentials and the number of password attempts can be controlled by administrators using the Centrify Group Policy settings. Please refer to Section 4.

The Password Prompt dialog will also show up anytime if Centrify PuTTY cannot find the destination machine using the provided Kerberos credentials. In this case the user needs to supply a different set of credentials. When this happens, the user can always check the **Remember my password** box so that he can silently access the same machine next time. Thus, Single Sign-on can be achieved in situations such as un-trusted forests or disjoint domains. The user can manage the cached passwords by invoking `control keymgr.dll` in a **Command** window.

Please note that in Windows 2000 machines, the **Remember my password** checkbox is not present when the user is prompted for credentials. Thus, Single Sign-on is not possible for Win2000 machines.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

4 Centrify PuTTY Group Policy Settings

Centrify provides a Group Object administrative template, `centrify_putty_settings.adm`, that allows centralized control of the configurable PuTTY settings including the Kerberos options for SSH connections. The Centrify PuTTY installer installs this template in the `c:\windows\inf` directory. Administrators who want to use the provided PuTTY group policies must copy this file to the appropriate domain controller machine. They can then configure settings to enhance users' PuTTY experience as well as to ensure more secure remote access.

This section will describe the Group Policy settings pertaining to Centrify's Kerberos authentication options only. For other configuration settings, please refer to the PuTTY documentation.

Many of the settings have been explained in Section 3.1. The following table provides a summary. Initially, all the configuration options are set to **Not Configured**. They can be set to **Enabled** to activate a policy setting or **Disabled** to disable a previously enabled setting. Policies with **Enabled** or **Disabled** settings will override policies applied earlier.

Configuration Parameter	**Value**	**Description**
Attempt Kerberos auth (SSH-2)	Radio button: • Not Configured • Enabled • Disabled When enabled, a checkbox to turn on the option.	Controls whether SSH should use Kerberos for authentication.
Create forwardable tickets	Radio button: • Not Configured • Enabled • Disabled When enabled, a checkbox to turn on the option.	Controls whether the same Kerberos credentials can be used for authentication to another SSH server.
Find machine from trusted domains	Radio button: • Not Configured • Enabled • Disabled When enabled, a checkbox to turn on the option.	Controls whether Centrify PuTTY can locate the target machine from trusted domains.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Configuration Parameter	**Value**	**Description**
Auto-login username	Radio button: • Not Configured • Enabled • Disabled When enabled, a drop down list box with the following values: • None • SAM account name • User name portion of UPN User principal name (require DirectControl)	Controls how the Unix account name should be provided to the SSH server on the destination machine.
Allow user to specify alternate Kerberos credentials	Radio button: • Not Configured • Enabled • Disabled When enabled, a checkbox to turn on the option.	Controls whether users can specify using alternate Kerberos credentials.
Allowed password entry attempts	Radio button: • Not Configured • Enabled • Disabled When enabled, an input text box with scroll bars to specify the number of attempts allowed.	Controls the number of time password attempts can be made when providing the Kerberos credentials. The default is 3.
Allow reverse DNS lookup	Radio button: • Not Configured • Enabled • Disabled When enabled, a checkbox to turn on the option.	Controls whether Centrify PuTTY should do a reverse DNS lookup if the user enters an IP address in the **Host Name (or IP address)** field on the first page (**Session**) of Putty. Since DNS servers may be compromised and return an incorrect Fully-Qualified Domain Name (FQDN), this provides administrators the option to turn on or off this facility.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Configuration Parameter	Value	Description
LDAP port of Active Directory domain controller	Radio button: • Not Configured • Enabled • Disabled When enabled, an input text box to specify the LDAP port.	Controls the port number to use if Centrify PuTTY has to set up an LDAP connection to Active Directory. The default is 389.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

5 PuTTY related utilities

Centrify has also enhanced **pscp.exe**, **psftp.exe** and **plink.exe** to support Kerberos authentication.

PSCP supports the following command formats

```
pscp [options] [user@]host:source target
pscp [options] source [source...] [user@]host:target
pscp [options] -ls [user@]host:filespec
```

PSFTP supports the following command formats

```
psftp [options] [user@]host
```

Plink supports the following command formats

```
plink [options] [user@]host [command]
```

Many of the PuTTY settings can be provided as options to the command line tools. In addition, users can save these settings into sessions and load them when executing the commands using the `-load` option. If the settings in a saved session conflict with those specified when invoking the command, specified options take precedence.

The Centrify PuTTY package adds several extra options to the above commands.

Option	Description
-k	Use Kerberos (GSS) authentication and provide a Unix user account name during login. This is equivalent to checking **Attempt Kerberos auth (SSH-2)** checkbox and selecting "**None**" as **Auto-login username** in the Centrify PuTTY Kerberos configuration page. Please refer to Section 3.1.
-K	Use Kerberos (GSS) authentication and do auto login. This is equivalent to checking both **Attempt Kerberos auth (SSH-2)** checkbox and selecting "**User principal name (requires DirectControl)**" as **Auto-login username** in the Centrify PuTTY Kerberos configuration page. Please refer to Section 3.1.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

Option	Description
-spn	Specify the Service Principal Name (SPN) of the target machine. The option takes effect only when –k or –K is used. This is equivalent to specifying the target's Service Principal Name in the "**Service principal name**" textbox in the Centrify PuTTY Kerberos configuration page. Please refer to Section 3.1.

Some Kerberos settings such as **Create forwardable ticket** and **Find machine from trusted domains** are not exposed as options to `PSCP.exe`, `PSFTP.exe` and `Plink.exe`. User can configure these settings using the Centrify PuTTY user interface, save them in a session and then load the session using the `-load` option.

5.1 Example

The following shows an example of how to use the Centrify enhanced PuTTY command line utility to facilitate administrative tasks. The command executed is:

```
pscp –K RedHatLinux:/etc/group c:\temp
```

In this example, the `\etc\group` file is retrieved from a remote Linux machine (RedHatLinux) using the `pscp.exe` utility. The "`-K`" option is used, meaning that the current user login name and credentials are used for Kerberos authentication to the remote machine. Note that by using this option, there is no need to specify a user name in the command line or be prompted for password during runtime. Hence, the command can be easily embedded in a batch file for administrative usage.

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.

6 References

For further information on PuTTY, please see the following documentation:

- PuTTY Home Page (http://www.chiark.greenend.org.uk/~sgtatham/putty/)
- PuTTY User Manual (http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html)

©2007 CENTRIFY CORPORATION. ALL RIGHTS RESERVED.