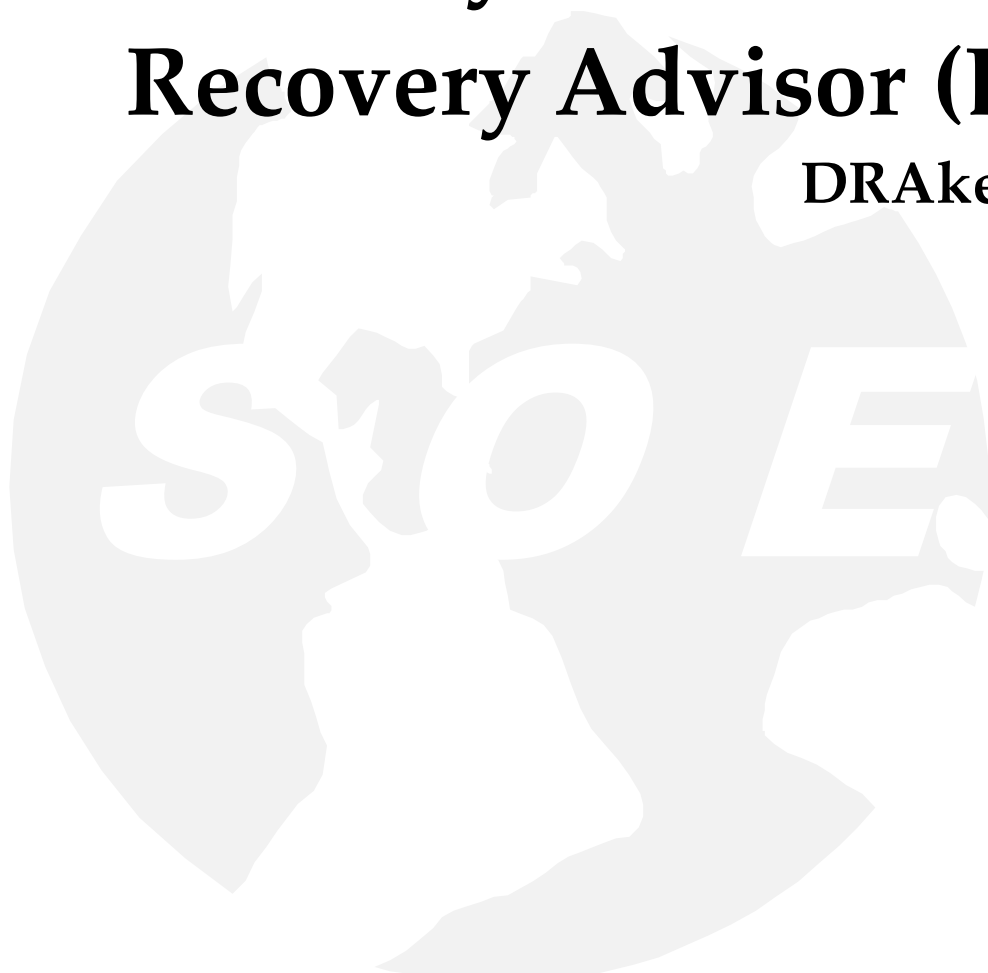




CATE CitiSystems High Availability Engineering

Symantec Disaster Recovery Advisor (DRA)

DRAkey 1.0-A3



Release for Production
Document Version 1.5

© Citigroup, Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside Citigroup is prohibited without express permission.

Table of Contents

TABLE OF CONTENTS	2
VERSION CONTROL.....	3
APPLICABILITY	3
CERTIFICATION MATRIX.....	3
PACKAGES AND CHECKSUMS	3
RFP – DRAKEY 1.0-A3	4
INTRODUCTION	4
INTENDED AUDIENCE.....	4
OVERVIEW	4
BENEFIT TO THE FIRM.....	4
KNOWN ISSUES	4
PREREQUISITES.....	4
TIME LINE.....	4
VERSION HISTORY	5
INSTALLING DRAKEY PACKAGE.....	5
UNINSTALLING DRAKEY PACKAGE.....	5
UPGRADING DRAKEY PACKAGE.....	5
NETWORK SERVICES AND LISTENERS.....	5
NETWORK PORT DETAILS.....	5
TESTING AND CERTIFICATION.....	5
TEST PROCEDURE AND RESULT	5
REFERENCES	5
APPENDIX A: DRAKEY RHEL INSTALLATION.....	6
APPENDIX B: DRAKEY SOLARIS INSTALLATION	6
APPENDIX C: DRAKEY AIX INSTALLATION	7
APPENDIX D: DRAKEY RHEL UNINSTALLATION	8
APPENDIX E: DRAKEY SOLARIS UNINSTALLATION	8
APPENDIX F: DRAKEY AIX UNINSTALLATION	9
APPENDIX G: DRAKEY UPGRADE FROM PREVIOUS DRAKEY VERSION.....	10
APPENDIX H: DRA MASTER SIDE SETUP	10

Version Control

Version		Date	Author	Comments
Product	Document			
1.0-A0	1.0	Nov 21, 2014	Vivek Kamat	Initial Release(RFT) of DRAkey
1.0-A0	1.0	Dec 15, 2014	Vivek Kamat	RFP.
1.0-A1	1.1	Jan 23, 2015	Vivek Kamat	Fix conflicts with drscan user on ldap for RHEL and Solaris. No changes in AIX package.
1.0-A2	1.2	Feb 06, 2015	Vivek Kamat	Removed user/group provisioning section.
1.0-A2	1.3	Feb 26, 2015	Surendra Nimje	RFP.
1.0-A3	1.4	Jul 07, 2015	Surendra Nimje	RFT. Added new collector FQDNs in the package.
1.0-A3	1.5	Aug 03, 2015	Surendra Nimje	RFP.

Applicability

Business/Region affected	Global
Requestor/VR number	
Planview Project Entry	CAT150061104
Platform	RHEL/AIX/Solaris
Operating system version	All CATE supported versions.
Security model tier	GSF
CAP	
VTM ID	
VTM TAPL	
GE Forum Thread	https://collaborate.citi.net/groups/cate-global-citi-systems-high-availability-engineering-team/blog/2014/09/03/dra-releases
Software location/package name	/net/stealth.nj.ssmb.com/export1/home1.localhost/sw/PKG/DRAkey.1.0_A3.dstream /net/stealth.nj.ssmb.com/export1/home1.localhost/sw/AIX/IHS.DRAkey.1.0.0.2.bff /net/stealth.nj.ssmb.com/export1/home1.localhost/sw/Linux/DRAkey-1.0-A3.noarch.rpm

Certification Matrix

Hardware	x86_64, SPARC, IBM pSeries
Software	DRA 6.3.2 and SSH Tectia 6.3

Packages and checksums

The following checksums were generated and may be validated using the tools available in RHEL and AIX server:

CRC32: /usr/bin/cksum <filename>

MD5SUM: /usr/bin/openssl md5 <filename>

The following checksums were generated and may be validated using the tools available in Solaris server:

MD5SUM: /bin/digest -a md5 <filename>

Package Name	TPM Package Name	Size(B)	CRC32	MD5SUM
DRAkey-1.0-A3.noarch.rpm	CITI_RedHat_DRAkey-1.0-A3.noarch_1.0	5006	214238919	f4f809318e961870d94f9238c1055597
IHS.DRAkey.1.0.0.2.bff	CITI_AIX_IHS.DRAkey.rte_1.0.0.2_1.0	7680	3034282549	a00b81cbc10f30b4b8a29b967a65214e
DRAkey.1.0_A3.dstream	CITI_Solaris_DRAkey_1.0_A3_1.0	9728	3648535815	2f3cffe4239d5eeb27977f412eb8d6d

RFP – DRAkey 1.0-A3

CATE CitiSystems High Availability Engineering – Surendra Nimje – Aug 03, 2015

Introduction

CATE CitiSystems High Availability Engineering is publishing the Release for Production of DRAkey version 1.0-A3. This version will add new collector FQDNs into the Unix/Linux host DRAkey package to allow the newly added collectors scanning the hosts.

Intended Audience

This document is intended for the Global SOE Task Force, Global Security communities and anyone with a vested interest in this solution. For further questions, please email CATE CitiSystems High Availability Engineering at [*CATE GLOBAL CitiSystems High Availability Engineering](mailto:CATE.GLOBAL@CitiSystems.com).

Overview

In an effort to find new ways to improve business & IT resiliency, Citigroup has engaged Symantec to perform a deployment of the Symantec Disaster Recovery Advisor™ product (from here on referred to as "the system" or "DRA"). DRA proactively monitors and automatically detects potentially threatening data protection and availability configuration risks that exist within the data center. The existence of such risks are the direct result of the volume of changes within the datacenter combined with complex provisioning processes that are implemented by cross functional teams within IT. It is impossible to prevent such errors given the nature of these environments. The need to automate discovery and proactively illuminate these irregularities before a disaster is critical to managing risk.

DRA host onboarding requires Unix/Linux host with FID, group and login credentials. Initial deployments used SSH keyboard authentication as credential to connect to the Unix/Linux host for scanning. This package will setup the SSH public key authentication securely for DRA master and collector servers for scanning. CMP provision should be used to create drscan id and group at LDAP or locally on the server before installing the package.

Benefit to the Firm

This version will automate the Unix/Linux host side requirements for DRA onboarding and will help to speedup the deployments.

Known Issues

- None.

Prerequisites

- FID drscan and group drscan should exist on the server either via LDAP or locally.
- UNIX servers should be able to DNS resolve DRA master and collectors. Only DRA master and Collector servers will be able to connect to drscan account.
- DRA master side setup (Refer [APPENDIX G](#) for detailed steps)
 - SSHtectia Client (CITI_WIN_TectiaSSHClient_638_00) on DRA master server.
 - Need to create a SSH User keys (Private and Public)
 - New host authentication credentials on DRA master.
 - New Connection Policy.

Time Line

Released for Integration/SA testing (RFT)	07th Jul 2015
Integration/SA testing completed	31 th Jul 2015
Production Release (RFP)	03 rd Aug 2015

Version History

1.0 Initial release

1.0 A1

fixes drascan conflict issue with LDAP for Solaris and RHEL.
For Linux used lgroupadd instead of groupadd.
Updated "gecos" field to reflect the current owner of the FID.

1.0 A2

drascan user and group provisioning section removed from the package.

1.0 A3

Adds new and reserved collector FQDNs into the DRAKey package.

Installing DRAkey package

[APPENDIX A for RHEL](#)

[APPENDIX B for Solaris](#)

[APPENDIX C for AIX](#)

Uninstalling DRAkey package

[APPENDIX D for RHEL](#)

[APPENDIX E for Solaris](#)

[APPENDIX F for AIX](#)

Upgrading DRAkey package

[APPENDIX G](#)

Network Services and Listeners

N/A

Network Port Details

Source		Destination		Direction
System	Port	System	Port	
DRA and All collectors	Ephemeral	Unix Servers(SSH server)	22/TCP	DRA(SSH Client) to Unix Server(SSH Server)

Testing and Certification

Test Procedure and Result

https://catecollaboration.citigroup.net/domains/platstor/osunix/stdsrelateddocs/DRAKey_1.0-A3_Test_Cases.xls

References

- **Link to Symantec Documentation:** https://sort.symantec.com/documents/doc_details/dra/6.1.1/Windows%20and%20UNIX/ProductGuides
- **CitiSystems Product Page:** <https://catecollaboration.citigroup.net/domains/platstor/osunix/default.aspx>

Appendix A: DRAkey RHEL Installation

```
# rpm -ivh DRAkey-1.0-A3.noarch.rpm
```

```
Preparing... ##### [100%]  
 1:DRAkey ##### [100%]  
#
```

Appendix B: DRAkey Solaris Installation

```
# pkgadd -d /var/tmp/DRAkey.1.0_A3.dstream DRAkey
```

```
Processing package instance <DRAkey> from </var/tmp/DRAkey.1.0_A3.dstream>
```

```
Symantec DRA PROD key package for Unix/Linux(sun4) 1.0_A3
```

```
Citigroup
```

```
## Executing checkinstall script.
```

```
## Processing package information.
```

```
## Processing system information.
```

```
## Verifying disk space requirements.
```

```
## Checking for conflicts with packages already installed.
```

```
## Checking for setuid/setgid programs.
```

```
Installing Symantec DRA PROD key package for Unix/Linux as <DRAkey>
```

```
## Installing part 1 of 1.
```

```
/etc/opt/SSHtecta/keys/drascan/authorization
```

```
/etc/opt/SSHtecta/keys/drascan/authorized_keys2
```

```
[ verifying class <none> ]
```

```
Installation of <DRAkey> was successful.
```

```
#
```

Appendix C: DRAkey AIX Installation

```
# installp -ad /var/tmp IHS.DRAkey.rte
+-----+
+           Pre-installation Verification...
+-----+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESES
-----
Filesets listed in this section passed pre-installation verification
and will be installed.

Selected Filesets
-----
IHS.DRAkey.rte  1.0.0.2          # Symantec DRA PROD key packag...

<< End of Success Section >>

+-----+
+           BUILDDATE Verification ...
+-----+
Verifying build dates...done
FILESET STATISTICS
-----
  1 Selected to be installed, of which:
    1 Passed pre-installation verification
  ---
  1 Total to be installed

+-----+
+           Installing Software...
+-----+

installp: APPLYING software for:
IHS.DRAkey.rte  1.0.0.2

Finished processing all filesets. (Total time:  1 secs).

+-----+
+           Summaries:
+-----+

Installation Summary
-----
Name                Level      Part      Event      Result
-----
IHS.DRAkey.rte      1.0.0.2    USR        APPLY      SUCCESS
#
```

Appendix D: DRAkey RHEL Uninstallation

```
# rpm -ev DRAkey
#
```

Appendix E: DRAkey Solaris Uninstallation

```
# pkgrm DRAkey
```

The following package is currently installed:

DRAkey Symantec DRA PROD key package for Unix/Linux
(sun4) 1.0_A3

Do you want to remove this package? [y,n,?,q] y

```
## Removing installed package instance <DRAkey>
```

This package contains scripts which will be executed with super-user permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y

```
## Verifying package <DRAkey> dependencies in global zone
```

```
## Processing package information.
```

```
## Removing pathnames in class <none>
```

```
/opt/drscan
```

```
/etc/opt/SSHtecta/keys/drscan/authorized_keys2
```

```
/etc/opt/SSHtecta/keys/drscan/authorization
```

```
/etc/opt/SSHtecta/keys/drscan
```

```
## Executing postremove script.
```

```
## Updating system information.
```

Removal of <DRAkey> was successful.

```
#
```

Appendix F: DRAkey AIX Uninstallation

```
# installp -u IHS.DRAkey.rte
+-----+
+           Pre-deinstall Verification...
+-----+
Verifying selections...done
Verifying requisites...done
Results...

SUCCESES
-----
Filesets listed in this section passed pre-deinstall verification
and will be removed.

Selected Filesets
-----
IHS.DRAkey.rte  1.0.0.2          # Symantec DRA PROD key packag...

<< End of Success Section >>

FILESET STATISTICS
-----
  1 Selected to be deinstalled, of which:
    1 Passed pre-deinstall verification
  ---
  1 Total to be deinstalled

+-----+
+           Deinstalling Software...
+-----+

installp: DEINSTALLING software for:
IHS.DRAkey.rte  1.0.0.2

Finished processing all filesets. (Total time:  0 secs).

+-----+
+           Summaries:
+-----+

Installation Summary
-----
Name                Level      Part      Event      Result
-----
IHS.DRAkey.rte      1.0.0.2    USR        DEINSTALL  SUCCESS
#
```

Appendix G: DRAKey upgrade from previous DRAkey version

- 1) Uninstall the previous version of DRAkey package from the host
- 2) Install the new DRAkey package

Appendix H: DRA Master side setup

- 1) Install TPM package CITI_WIN_TectiaSSHClient_638_00
- 2) Generate the keypair using the following steps.
 - a. Launch the command prompt using “run as administrator”
 - b. CD c:\apps_srv\sshtectia\scripts
 - c. Run the script Keypairgen.cmd
 - i. Domain : NAM
 - ii. Functional account: drascan
- 3) Public and Private key saved to c:\APPS_SRV\SSHtectia\keys\drascan\
- 4) Run the following command to convert the SSH private key to OpenSSH format. DRA supports only OpenSSH keys.
 - a. ssh-keygen-g3--key-format openssh2--import-private-key id_dsa_2048_a id_dsa_openssh
 - b. this will create a new file id_dsa_openssh
- 5) Create a new credential using DRA UI Eg: drascan-sshkey as follows.
 - a. Credential type : SSH – Publickey Authentication.
 - b. Description: drascan-sshkey
 - c. Username: drascan
 - d. Password : keep blank
 - e. PEM Private key : browse to the openssh private key file generated in the first step.
- 6) Create Policy as Usual, except use credential created in the steps 5.