Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 8/20

(Certification No.)

Prodotto: Nutanix Enterprise Cloud (AOS & AHV) v5.15

(Product)

Sviluppato da: Nutanix, Inc.

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL2+

(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente
da Eva Spina
Data: 2020.10.09
10:28:31 +02'00'

Roma, 9 ottobre 2020

Common Criteria

SOGIS IT SECURITY CERTIFIED

Questa pagina è lasciata intenzionalmente vuota

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Rapporto di Certificazione

Nutanix Enterprise Cloud (AOS & AHV) v5.15

OCSI/CERT/CCL/01/2020/RC

Versione 1.0

9 ottobre 2020

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	09/10/2020

2 Indice

3 Elenco degli acronimi

AHV	Acropolis Hypervisor
AJAX	Asynchronous JavaScript and XML
AOS	Acropolis Operating System
API	Application Programming Interface
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CSRF	Cross-site Request Forgery
CVM	Controller Virtual Machine
EAL	Evaluation Assurance Level
HDD	Hard Disk Drive
HW	Hardware
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
nCLI	Nutanix Command Line Interface
NFS	Network File System
NIS	Nota Informativa dello Schema
NTP	Network Time Protocol
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OLE	Object Linking and Embedding
OPC	OLE for Process Control

OS	Operating System
PCIe	Peripheral Component Interconnect Express
PP	Protection Profile
REST	Representational State Transfer
RFV	Rapporto Finale di Valutazione
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SOGIS	Senior Officials Group Information Systems Security
SOGIS-MRA	SOGIS – Mutual Recognition Arrangement
SSD	Solid-state Drive
SSH	Secure Shell
ST	Security Target
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
XML	eXtensible Markup Language

4 Riferimenti

4.1 Criteri e normative

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Documenti tecnici

[AA] Nutanix AOS 5.15 Acropolis Advanced Administration Guide, Nutanix, Inc., 31 March 2020

[AG] Nutanix AHV 5.15 AHV Administration Guide, Nutanix, Inc., 31 March 2020

[AGD] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Guidance Documentation Supplement; Evaluation Assurance Level (EAL): EAL2+, v0.3, Nutanix, Inc., 16 July 2020

[API] Nutanix AOS 5.10 Acropolis v1 API Reference, Nutanix, Inc., 31 March 2020

[AS] Nutanix AOS 5.15 Acropolis Advanced Setup Guide, Nutanix, Inc., 31 March 2020

[CMC] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Configuration Management Document; Evaluation Assurance Level (EAL): EAL2+, v0.4, Nutanix, Inc., 24 September 2020

[CR] Nutanix AOS 5.15 Command Reference, Nutanix, Inc., 31 March 2020

[DEL] Nutanix Enterprise Cloud (AOS & AHV) v5.15 Secure Delivery Document; Evaluation Assurance Level (EAL): EAL2+, v0.1, Nutanix, Inc., 25 March 2020

[GS] Nutanix AOS 5.15 Acropolis Getting Started Guide NX Series, March 31, 2020

[NS] Nutanix Security 5.15 Security Guide, Nutanix, Inc., 31 March 2020

[RFV] “Nutanix Enterprise Cloud (AOS & AHV) v5.15” Evaluation Technical Report, v.3, CCLab Software Laboratory, 23 September 2020

[TDS] “Nutanix Enterprise Cloud (AOS & AHV) v5.15” Security Target, Nutanix, Inc., Version 0.7, 17 July 2020

[WP] Nutanix Prism 5.15 Prism Web Console Guide, Nutanix, Inc., 31 March 2020

5 Riconoscimento del certificato

5.1 Riconoscimento di certificati CC in ambito europeo (SOGIS-MRA)

L'accordo di mutuo riconoscimento in ambito europeo (SOGIS-MRA, versione 3, [SOGIS]) è entrato in vigore nel mese di aprile 2010 e prevede il riconoscimento reciproco dei certificati rilasciati in base ai Common Criteria (CC) per livelli di valutazione fino a EAL4 incluso per tutti i prodotti IT. Per i soli prodotti relativi a specifici domini tecnici è previsto il riconoscimento anche per livelli di valutazione superiori a EAL4.

L'elenco aggiornato delle nazioni firmatarie e dei domini tecnici per i quali si applica il riconoscimento più elevato e altri dettagli sono disponibili su https://www.sogis.eu/.

Il logo SOGIS-MRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito SOGIS-MRA per tutti i componenti di garanzia selezionati.

5.2 Riconoscimento di certificati CC in ambito internazionale (CCRA)

La versione corrente dell'accordo internazionale di mutuo riconoscimento dei certificati rilasciati in base ai CC (Common Criteria Recognition Arrangement, [CCRA]) è stata ratificata l'8 settembre 2014. Si applica ai certificati CC conformi ai Profili di Protezione "collaborativi" (cPP), previsti fino al livello EAL4, o ai certificati basati su componenti di garanzia fino al livello EAL2, con l'eventuale aggiunta della famiglia Flaw Remediation (ALC_FLR).

L'elenco aggiornato delle nazioni firmatarie e dei Profili di Protezione "collaborativi" (cPP) e altri dettagli sono disponibili su https://www.commoncriteriaportal.org/.

Il logo CCRA stampato sul certificato indica che è riconosciuto dai paesi firmatari secondo i termini dell'accordo.

Il presente certificato è riconosciuto in ambito CCRA per tutti i componenti di garanzia selezionati.

6 Dichiarazione di certificazione

L'oggetto della valutazione (ODV) è il prodotto software "Nutanix Enterprise Cloud (AOS & AHV) v.5.15", nel seguito del documento anche indicato come "Nutanix Enterprise Cloud v5.15", sviluppato da Nutanix, Inc.

L'ODV è una piattaforma di virtualizzazione in grado di ospitare macchine virtuali (VM) che offrono servizi e archiviazione agli utenti (tipicamente come server virtuali) come servizi Web, posta elettronica o altro. Inoltre, l'ODV è scalabile in modo lineare per soddisfare le accresciute esigenze di elaborazione o archiviazione dei server virtuali, consentendo l'aggiunta di singoli nodi ulteriori al cluster, il che riduce notevolmente le esigenze hardware rispetto a un'infrastruttura server tradizionale.

La valutazione è stata condotta in accordo ai requisiti stabiliti dallo Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione ed espressi nelle Linee Guida Provvisorie [LGP1, LGP2, LGP3] e nelle Note Informative dello Schema [NIS1, NIS2, NIS3]. Lo Schema è gestito dall'Organismo di Certificazione della Sicurezza Informatica, istituito con il DPCM del 30 ottobre 2003 (G.U. n.98 del 27 aprile 2004).

Obiettivo della valutazione è fornire garanzia sull'efficacia dell'ODV nel rispettare quanto dichiarato nel Traguardo di Sicurezza [TDS], la cui lettura è consigliata ai potenziali acquirenti e/o utilizzatori. Le attività relative al processo di valutazione sono state eseguite in accordo alla Parte 3 dei Common Criteria [CC3] e alla Common Evaluation Methodology [CEM].

L'ODV è risultato conforme ai requisiti della Parte 3 dei CC v 3.1 per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in conformità a quanto riportato nel Traguardo di Sicurezza [TDS] e nella configurazione riportata in Appendice B – Configurazione valutata di questo Rapporto di Certificazione.

La pubblicazione del Rapporto di Certificazione è la conferma che il processo di valutazione è stato condotto in modo conforme a quanto richiesto dai criteri di valutazione Common Criteria – ISO/IEC 15408 ([CC1], [CC2], [CC3]) e dalle procedure indicate dal Common Criteria Recognition Arrangement [CCRA] e che nessuna vulnerabilità sfruttabile è stata trovata. Tuttavia l'Organismo di Certificazione con tale documento non esprime alcun tipo di sostegno o promozione dell'ODV.

7 Riepilogo della valutazione

7.1 Introduzione

Questo Rapporto di Certificazione specifica l'esito della valutazione di sicurezza del prodotto "Nutanix Enterprise Cloud (AOS & AHV) v.5.15" secondo i Common Criteria, ed è finalizzato a fornire indicazioni ai potenziali acquirenti e/o utilizzatori per giudicare l'idoneità delle caratteristiche di sicurezza dell'ODV rispetto ai propri requisiti.

Il presente Rapporto di Certificazione deve essere consultato congiuntamente al Traguardo di Sicurezza [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente previsto.

7.2 Identificazione sintetica della valutazione

Nome dell'ODV	Nutanix Enterprise Cloud (AOS & AHV) v.5.15
Traguardo di sicurezza	"Nutanix Enterprise Cloud (AOS & AHV) v5.15" Security Target, Version 0.7 [TDS]
Livello di garanzia	EAL2 con l'aggiunta di ALC_FLR.2
Fornitore	Nutanix, Inc.
Committente	Nutanix, Inc.
LVS	CCLab Software Laboratory
Versione dei CC	3.1 Rev. 5
Conformità a PP	Nessuna conformità dichiarata
Data di inizio della valutazione	15 gennaio 2020
Data di fine della valutazione	23 settembre 2020

I risultati della certificazione si applicano unicamente alla versione del prodotto indicata nel presente Rapporto di Certificazione e a condizione che siano rispettate le ipotesi sull'ambiente descritte nel Traguardo di Sicurezza [TDS].

7.3 Prodotto valutato

In questo paragrafo vengono sintetizzate le principali caratteristiche funzionali e di sicurezza dell'ODV; per una descrizione dettagliata, si rimanda al Traguardo di Sicurezza [TDS].

L'ODV "Nutanix Enterprise Cloud v5.15" è un software che fornisce le funzionalità di sicurezza definite di seguito. L'ODV comprende tutto il software Nutanix che costituisce Nutanix Enterprise Cloud in un cluster a tre host. Tutto l'hardware necessario per il funzionamento dell'ODV è considerato parte dell'ambiente operativo dell'ODV.

L'ODV è costituito dai seguenti componenti software:

- Acropolis Operating System (AOS) v5.15 LTS.
- Acropolis Hypervisor (AHV) v20170830.395.

L'ODV applica una politica di sicurezza per l'accesso ai dischi virtuali (Virtual Disk Access SFP) sulle VM ospitate dall'ODV. Questa SFP controlla l'accesso delle VM ospiti allo spazio di archiviazione fornito dall'ODV. Per determinare se una VM ospite può accedere a un disco virtuale, l'ODV controlla prima una whitelist NFS e quindi controlla se la VM ospite è stata configurata per accedere alla condivisione NFS.

L'ODV applica una politica di sicurezza per il lock dei dischi virtuali (Virtual Disk Locking SFP) sui client che tentano di scrivere o eseguire file archiviati su dischi virtuali. Questa SFP consente un'operazione di lettura o di esecuzione se il processo che richiede l'operazione ha ottenuto un lock del disco virtuale. Se al momento della richiesta di accesso sul disco virtuale non è già presente un lock, l'ODV consente al processo di richiedere un lock del disco virtuale. In caso contrario, la richiesta di operazione viene negata.

L'ODV genera record di audit per tutte le modifiche alla configurazione apportate tramite le interfacce di gestione. All'interno di questi record di audit, l'ODV include informazioni di base sull'evento in un formato leggibile dall'uomo. L'ODV fornisce marche temporali affidabili che vengono utilizzate per preservare l'ordine degli eventi per i record di audit.

L'ODV include una serie di interfacce di gestione utilizzabili dagli utenti amministrativi per visualizzare i log di audit, configurare la funzionalità di failover, gestire le impostazioni dell'ODV, gestire gli account e configurare la funzione di archiviazione fornita dall'ODV. Le interfacce di gestione possono essere utilizzate anche per configurare la SFP per l'accesso ai dischi virtuali e la SFP di lock dei dischi virtuali. Le opzioni di archiviazione includono il tipo di accesso (pass-through o formato disco virtuale), le opzioni di tiering (SSD PCIe, SSD o HDD) e la capacità massima allocata. Esistono tre ruoli amministrativi definiti per l'ODV: amministratore utenti (User Administrator), amministratore cluster (Cluster Adminstrator) e sola visualizzazione (View Only). Gli utenti amministratori possono disconnettersi dalle proprie sessioni di gestione in qualsiasi momento.

L'ODV richiede che gli utenti amministrativi effettuino l'identificazione e l'autenticazione prima di accedere a qualsiasi funzionalità dell'ODV. Durante l'autenticazione tramite Prism, all'utente amministrativo viene fornito solo feedback oscurato. L'ODV conserva anche le password per gli account locali e i nomi utente associati.

7.3.1 Architettura dell'ODV

All'interno del confine dell'ODV sono inclusi i componenti AOS e AHV sviluppati da Nutanix per la distribuzione su tre host del Nutanix Enterprise Cloud. Sono considerati software dell'ODV anche le parti di codice sorgente o il software di terze parti modificato da Nutanix per Nutanix Enterprise Cloud.

Il confine dell'ODV non include i seguenti componenti dell'ambiente operativo mostrati nella Figura 1:

- VM ospiti in esecuzione su AHV;

- workstation;
- hardware, telaio, o dischi dell'host;
- server NTP.

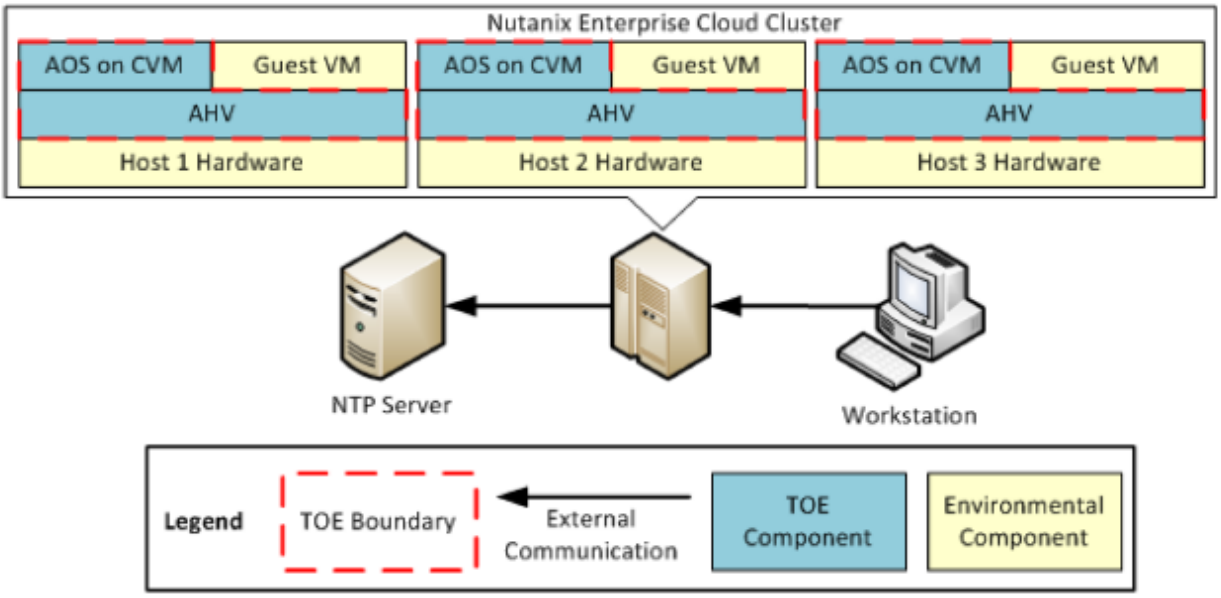

Figura 1 – Confini dell'ODV

I seguenti componenti non sono mostrati in Figura 1 e sono considerati parte dell'ambiente operativo dell'ODV:

- client nCLI locali in esecuzione sulla workstation;
- client REST API in esecuzione sulla workstation;
- browser Web in esecuzione sulla workstation;
- strumenti di gestione o prodotti utilizzati per accedere all'AHV.

7.3.2 Caratteristiche di sicurezza dell'ODV

Il problema di sicurezza dell'ODV, comprendente obiettivi di sicurezza, ipotesi, minacce e politiche di sicurezza dell'organizzazione, è definito nel cap. 3 del Traguardo di Sicurezza [TDS].

Per una descrizione dettagliata delle Funzioni di Sicurezza dell'ODV, si consulti il par. 7.1 del Traguardo di Sicurezza [TDS]. Gli aspetti più significativi sono riportati qui di seguito:

- **Audit di Sicurezza**: l'ODV registra le azioni degli utenti amministrativi eseguite attraverso le interfacce di gestione. I record di audit possono essere esaminati solo attraverso Prism.
- **Protezione dei Dati d'Utente**: l'ODV impone controlli di accesso allo storage allocato alle VM. Gli spazi di archiviazione sono forniti tramite condivisioni NFSv4.

L'accesso allo storage è controllato tramite una whitelist NFS che elenca l'indirizzo IP di ogni VM ospite a cui è consentito accedere allo spazio di archiviazione. L'ODV fornisce anche controlli sulle informazioni tali che solo un client alla volta possa modificare i dati di un disco virtuale.

- **Identificazione ed Autenticazione**: l'ODV richiede agli utenti di identificarsi e autenticarsi prima di concedere l'autorizzazione ad accedere a qualsiasi funzionalità dell'ODV stesso. Gli utenti amministratori devono utilizzare password complesse. L'ODV memorizza il nome utente e la password di ogni account locale. Effettuando l'accesso a Prism, l'ODV oscura le password per gli utenti amministrativi.

- **Gestione della Sicurezza**: l'ODV fornisce le interfacce API REST, Prism e nCLI che possono essere utilizzate dagli utenti amministrativi per gestire l'ODV. Tramite queste interfacce gli amministratori possono gestire gli attributi di sicurezza relativi alla politica di accesso ai dischi virtuali. Questa SFP consente di effettuare qualsiasi richiesta di accesso allo spazio di archiviazione per impostazione predefinita, a meno che un disco virtuale non sia già in lock. Gli utenti amministrativi possono anche gestire account, container, archiviazione, dischi virtuali e server NTP. Gli amministratori possono assumere il ruolo di User Administrator, il ruolo di Cluster Administrator, il ruolo View Only o possono ottenere insiemi multipli di privilegi contemporaneamente.

- **Protezione del TSF**: l'ODV mantiene le sue piene capacità quando un disco fisico o un host si guasta.

- **Utilizzo delle Risorse**: l'ODV fa uso di host ridondanti per prevenire un single point of failure. L'ODV rimane completamente operativo con tutti i dati intatti anche se un intero disco fisico o host si guasta.

- **Accesso all'ODV**: l'ODV offre agli utenti amministratori la possibilità di disconnettersi da Prism e nCLI.

7.4 Documentazione

La documentazione specificata in Appendice A – Indicazioni per l'uso sicuro del prodotto, viene fornita al cliente insieme al prodotto.

La documentazione indicata contiene le informazioni richieste per l'inizializzazione, la configurazione e l'utilizzo sicuro dell'ODV in accordo a quanto specificato nel Traguardo di Sicurezza [TDS].

Devono inoltre essere seguite le ulteriori raccomandazioni per l'utilizzo sicuro dell'ODV contenute nel par. 8.2 di questo rapporto.

7.5 Conformità a profili di protezione

Il Traguardo di Sicurezza [TDS] non dichiara conformità ad alcun Profilo di Protezione.

7.6 Requisiti funzionali e di garanzia

Tutti i Requisiti di Garanzia (SAR) sono stati selezionati dai CC Parte 3 [CC3].

Tutti i Requisiti Funzionali (SFR) sono stati derivati dai CC Parte 2 [CC2].

Il Traguardo di Sicurezza [TDS], a cui si rimanda per la completa descrizione, specifica per l'ODV tutti gli obiettivi di sicurezza, le minacce che questi obiettivi devono contrastare, i Requisiti Funzionali di Sicurezza (SFR) e le funzioni di sicurezza che realizzano gli obiettivi stessi.

7.7 Conduzione della valutazione

La valutazione è stata svolta in conformità ai requisiti dello Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione, come descritto nelle Linee Guida Provvisorie [LGP3] e nelle Note Informative dello Schema [NIS3], ed è stata inoltre condotta secondo i requisiti del Common Criteria Recognition Arrangement [CCRA].

Lo scopo della valutazione è quello di fornire garanzie sull'efficacia dell'ODV nel soddisfare quanto dichiarato nel rispettivo Traguardo di Sicurezza [TDS], di cui si raccomanda la lettura ai potenziali acquirenti. Inizialmente è stato valutato il Traguardo di Sicurezza per garantire che costituisse una solida base per una valutazione nel rispetto dei requisiti espressi dallo standard CC. Quindi è stato valutato l'ODV sulla base delle dichiarazioni formulate nel Traguardo di Sicurezza stesso. Entrambe le fasi della valutazione sono state condotte in conformità ai CC Parte 3 [CC3] e alla CEM [CEM].

L'Organismo di Certificazione ha supervisionato lo svolgimento della valutazione eseguita dall'LVS CCLab Software Laboratory.

L'attività di valutazione è terminata in data 23 settembre 2020 con l'emissione, da parte dell'LVS, del Rapporto Finale di Valutazione [RFV] che è stato approvato dall'Organismo di Certificazione il 24 settembre 2020. Successivamente, l'Organismo di Certificazione ha emesso il presente Rapporto di Certificazione.

7.8 Considerazioni generali sulla validità della certificazione

La valutazione ha riguardato le funzionalità di sicurezza dichiarate nel Traguardo di Sicurezza [TDS], con riferimento all'ambiente operativo ivi specificato. La valutazione è stata eseguita sull'ODV configurato come descritto in Appendice B – Configurazione valutata. I potenziali acquirenti sono invitati a verificare che questa corrisponda ai propri requisiti e a prestare attenzione alle raccomandazioni contenute in questo Rapporto di Certificazione.

La certificazione non è una garanzia di assenza di vulnerabilità; rimane una probabilità (tanto minore quanto maggiore è il livello di garanzia) che possano essere scoperte vulnerabilità sfruttabili dopo l'emissione del certificato. Questo Rapporto di Certificazione riflette le conclusioni dell'Organismo di Certificazione al momento della sua emissione. Gli acquirenti (potenziali e effettivi) sono invitati a verificare regolarmente l'eventuale insorgenza di nuove vulnerabilità successivamente all'emissione di questo Rapporto di Certificazione e, nel caso le vulnerabilità possano essere sfruttate nell'ambiente operativo dell'ODV, verificare presso il produttore se siano stati messi a punto aggiornamenti di sicurezza e se tali aggiornamenti siano stati valutati e certificati.

8 Esito della valutazione

8.1 Risultato della valutazione

A seguito dell'analisi del Rapporto Finale di Valutazione [RFV] prodotto dall'LVS e dei documenti richiesti per la certificazione, e in considerazione delle attività di valutazione svolte, come testimoniato dal gruppo di Certificazione, l'OCSI è giunto alla conclusione che l'ODV "Nutanix Enterprise Cloud (AOS & AHV) v.5.15" soddisfa i requisiti della parte 3 dei Common Criteria [CC3] previsti per il livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2, in relazione alle funzionalità di sicurezza riportate nel Traguardo di Sicurezza [TDS] e nella configurazione valutata, riportata in Appendice B – Configurazione valutata.

La Tabella 1 riassume i verdetti finali di ciascuna attività svolta dall'LVS in corrispondenza ai requisiti di garanzia previsti in [CC3], relativamente al livello di garanzia EAL2, con l'aggiunta di ALC_FLR.2.

Classi e componenti di garanzia		**Verdetto**
Security Target evaluation	**Classe ASE**	Positivo
Conformance claims	ASE_CCL.1	Positivo
Extended components definition	ASE_ECD.1	Positivo
ST introduction	ASE_INT.1	Positivo
Security objectives	ASE_OBJ.2	Positivo
Derived security requirements	ASE_REQ.2	Positivo
Security Problem Definition	ASE_SPD.1	Positivo
TOE summary specification	ASE_TSS.1	Positivo
Development	**Classe ADV**	Positivo
Security architecture description	ADV_ARC.1	Positivo
Security-enforcing functional specification	ADV_FSP.2	Positivo
Basic design	ADV_TDS.1	Positivo
Guidance documents	**Classe AGD**	Positivo
Operational user guidance	AGD_OPE.1	Positivo
Preparative procedures	AGD_PRE.1	Positivo
Life cycle support	**Classe ALC**	Positivo
Use of a CM system	ALC_CMC.2	Positivo
Parts of the TOE CM coverage	ALC_CMS.2	Positivo
Flaw reporting procedures	*ALC_FLR.2*	Positivo
Delivery procedures	ALC_DEL.1	Positivo
Tests	**Classe ATE**	Positivo

Classi e componenti di garanzia		Verdetto
Evidence of coverage	ATE_COV.1	Positivo
Functional testing	ATE_FUN.1	Positivo
Independent testing – sample	ATE_IND.2	Positivo
Vulnerability assessment	**Classe AVA**	Positivo
Vulnerability analysis	AVA_VAN.2	Positivo

Tabella 1 – Verdetti finali per i requisiti di garanzia

8.2 Raccomandazioni

Le conclusioni dell'Organismo di Certificazione sono riassunte nel capitolo 6 (Dichiarazione di certificazione).

Si raccomanda ai potenziali acquirenti del prodotto "Nutanix Enterprise Cloud (AOS & AHV) v.5.15" di comprendere correttamente lo scopo specifico della certificazione leggendo questo Rapporto in riferimento al Traguardo di Sicurezza [TDS].

L'ODV deve essere utilizzato in accordo agli Obiettivi di Sicurezza per l'ambiente operativo specificati nel par. 4.2 del Traguardo di Sicurezza [TDS]. Si assume che, nell'ambiente operativo in cui è posto in esercizio l'ODV, vengano rispettate le Politiche di sicurezza organizzative e le ipotesi descritte rispettivamente nel par. 3.1 e nel par. 3.2 del Traguardo di Sicurezza [TDS].

Il presente Rapporto di Certificazione è valido esclusivamente per l'ODV nella configurazione valutata, in particolare in Appendice A – Indicazioni per l'uso sicuro del prodotto sono incluse alcune raccomandazioni relative alla consegna, all'inzializzazione e e utilizzo sicuro del prodotto, secondo le indicazioni contenute nella documentazione operativa fornita insieme all'ODV ([AA], [AG], [AGD], [AS], [CMC], [CR], [DEL], [GS], [NS], [WP], [API]).

9 Appendice A – Indicazioni per l'uso sicuro del prodotto

La presente appendice riporta considerazioni particolarmente rilevanti per il potenziale acquirente del prodotto.

9.1 Consegna

Il documento Secure Delivery Document [DEL] fornisce informazioni sulla consegna del prodotto e su come controllare il prodotto dopo averlo ricevuto.

Sono previste due possibilità: o acquistare l'ODV solo come software, quindi installarlo e configurarlo su hardware già disponibile, oppure ordinarlo insieme all'appliance hardware dallo sviluppatore.

Se il prodotto acquistato è solo software, l'ODV può essere scaricato dal sito Web del Fornitore. In questo caso, l'acquirente può verificare che il software sia originale confrontando il suo checksum SHA-256 con quello indicato nella pagina di download.

Se il prodotto viene consegnato come hardware + software, è possibile verificare il numero di tracciamento (UPS o FEDEX) e la lista dei componenti ordinati e spediti (dalla fattura) per assicurarsi che sia il prodotto originale. Una volta che l'hardware è stato installato e avviato, la versione del software (ODV) può essere verificata all'interno di Prism.

9.2 Installazione, initializzazione e utilizzo sicuro dell'ODV

Il documento Getting Started Guide [GS] fornisce informazioni sui passi necessari per preparare ed avviare l'ODV. La documentazione descrive la procedura per diverse configurazioni hardware (ad esempio, 1U1N, 2U4N). Il documento Administration Guide [AG] consiglia un minimo di 3 nodi per creare un cluster. Ulteriori dettagli sono forniti nel supplemento alla documentazione di guida [AGD] per la configurazione 2U3N. Tutte le procedure utente necessarie per preparare in modo sicuro l'ODV e il suo ambiente operativo sono descritte in [GS], [AG], [NS] e [AGD].

È necessario separare il traffico di gestione dal traffico di replica dell'archivizione (o backplane) creando un segmento di rete separato (LAN) per la replica dello storage, come descritto nel documento Nutanix Security Guide [NS].

Per un utilizzo sicuro dell'ODV, si rimanda ai documenti [AA], [AG], [CR], [WP] e [API].

10 Appendice B – Configurazione valutata

L'ODV è stato valutato nella configurazione descritta nel par. 1.6.1 del Traguardo di Sicurezza [TDS] e sintetizzata nel par. 7.3.1. Ulteriori dettagli sono forniti sull'ambiente HW per l'ODV in questo capitolo.

L'ambito fisico dell'ODV include i seguenti componenti software:

- AOS v5.15 LTS
- AHV v20170830.395.

La configurazione valutata dell'ODV è stata testata sulla piattaforma hardware NX-1365-G7 con Nutanix Enterprise Cloud 5.15.

Si evidenzia che la piattaforma NX-1365-G7 è equivalente alla NX-1065-G7, dove il "3" al posto dello "0" indica che ci sono 3 nodi nel telaio. Pur non essendovi stato testato, Nutanix Enterprise Cloud è in grado di funzionare anche su altre piattaforme hardware ed è derivato da una singola immagine con diverse funzionalità abilitate o disabilitate per supportare l'hardware specifico dell'host. Le seguenti piattaforme hardware possono essere utilizzate con il software dell'ODV:

- NX-1065-G7, NX-1175S-G7, NX-3060-G7, NX-3155-G7, NX-3170-G7, NX-8170-G7, NX-8150-G7, NX-8155-G7, NX -8035-G7, DX360-4-G10, DX360-8-G10, DX360-10-G10-NVMe, DX380-8-G10, DX380-12-G10, DX380-24-G10, DX560-24-G10, DX2200 -DX170R-G10-12LFF, DX2200-DX190R-G10-12LFF, DX2600-DX170R-G10-24SFF, DX4200-G10-24LFF, DX8000-DX910.

11 Appendice C – Attività di test

Questa appendice descrive l'impegno dei Valutatori e del Fornitore nelle attività di test. Per il livello di garanzia EAL2, con aggiunta di ALC_FLR.2, tali attività prevedono tre passi successivi:

- valutazione in termini di copertura e livello di approfondimento dei test eseguiti dal Fornitore;
- esecuzione di test funzionali indipendenti da parte dei Valutatori;
- esecuzione di test di intrusione da parte dei Valutatori.

11.1 Configurazione per i test

L'ambiente di test utilizzato è costituito da un ambiente fisico e uno virtuale. L'ambiente fisico è composto da un'appliance Nutanix, una workstation e da dispositivi di rete. I componenti AHV e AOS hanno richiesto la pre-configurazione per i test come definito nella documentazione di test del Fornitore. L'ambiente virtuale per i test consta di tre VM, ognuna predisposta con il sistema operativo Ubuntu installato e con un account super user. Per testare Prism è stato sufficiente utilizzare solo un browser su una workstation, mentre per testare le API REST, è stato necessario installare il software Postman sulla workstation. È stato anche necessario scaricare il client nCLI da Prism.

Prima dell'esecuzione dei test, i Valutatori hanno esaminato il piano di test per verificare che la configurazione di test dell'ODV fosse coerente con la documentazione del Fornitore, come anche dettagliato nei paragrafi 1.4 e 1.6.1 del Traguardo di Sicurezza [TDS].

La documentazione di test del Fornitore include istruzioni e descrizioni sufficientemente dettagliate per identificare qualsiasi dipendenza nell'ordine di esecuzione dei test e tutti i test elencati includono i risultati attesi.

11.2 Test funzionali svolti dal Fornitore

11.2.1 Approccio adottato per i test

I Valutatori hanno verificato che la documentazione dei test includesse i piani di test, i risultati attesi dei test e i risultati reali dei test. Sono stati predisposti i seguenti scenari di test:

- Scenario di Test 01: Test di Identificazione e Autenticazione.
- Scenario di Test 02: Test di Audit di Sicurezza.
- Scenario di Test 03: Test di Gestione della Sicurezza.
- Scenario di Test 04: Protezione dei Dati Utente.

- Scenario di Test 05: Protezione dei Dati Utente (Controllo del Flusso di Informazioni).

- Scenario di Test 06: Malfunzionamento dell'Host.

Gli scenari sono stati definiti per coprire tutti gli SFR e sono stati tutti testati esternamente e manualmente. Il piano di test menziona anche alcuni prerequisiti per l'hardware con una guida dettagliata su come preparare l'ODV per i test. La preparazione include il completamento dei passaggi descritti in [AGD], il caricamento di un'immagine disco, la creazione di macchine virtuali e l'installazione del sistema operativo su di esse, l'installazione dell'applicazione Postman e altri passaggi di configurazione. Ogni passaggio è stato descritto con dettagli sufficienti per garantire che la preparazione dei test e i test stessi fossero riproducibili.

11.2.2 Copertura dei test

I Valutatori hanno verificato che la corrispondenza tra i test identificati nella documentazione dei test e le TSFI descritte nelle specifiche funzionali fosse accurata.

Tutte le TSFI identificate nelle specifiche funzionali sono state incluse negli scenari di test predisposti:

1. Prism: fornisce un'interfaccia grafica Web basata su AJAX per la gestione remota del sistema cloud AHV e AOS.

2. nCLI: fornisce un'interfaccia a riga di comando basata su testo utilizzata anche in remoto da una workstation per gestire l'ODV.

3. API REST: fornisce un'interfaccia di programmazione, anche per gestire in remoto l'ODV tramite chiamate API.

4. Interfaccia di accesso all'archiviazione: è un'interfaccia di accesso ai dati che fornisce l'accesso alle condivisioni NFS e ai dischi virtuali.

11.2.3 Risultati dei test

I Valutatori hanno verificato che nella documentazione di test i risultati reali fossero coerenti con i risultati attesi.

L'esecuzione dello scenario di test 01 ha dimostrato che i dati di configurazione sono stati replicati nel cluster quando è stato effettuato un tentativo di disabilitare le CVM.

Lo scopo dello scenario di test 02 è stato quello di verificare la funzionalità di controllo di sicurezza dell'ODV tramite Prism, nCLI e l'API REST. È stato verificato che i record di audit fossero replicati sugli altri host nel cluster quando la VM è stata spenta o quando è stata creata ed eliminata una VM clonata.

Lo scenario di test 03 ha consentito di verificare l'applicazione degli SFR di gestione della sicurezza dimostrando che un utente amministrativo può fornire spazio di archiviazione, gestire gli account utente e modificare le impostazioni NTP (Network Time Protocol). Durante l'esecuzione del test è stata spenta una CVM per verificare che l'ODV replicasse i dati di gestione sulle altre CVM nel cluster.

Lo scenario di test 04 ha consentito di verificare l'interfaccia di accesso alla funzione di archiviazione, mostrando che gli utenti possono accedere all'archiviazione in una condivisione NFS e che l'accesso non è consentito per impostazione predefinita. Durante l'esecuzione del test è stato rimosso un disco rigido dal telaio del server per simulare un guasto del disco e forzare l'ODV a fornire i dati memorizzati tramite l'interfaccia di richiesta dati (Data Request).

Lo scopo dello scenario di test 05 è stato quello di verificare che la funzionalità di lock del disco fornita dall'ODV controllasse il flusso di informazioni ai dischi virtuali dalle VM ospiti. Durante l'esecuzione del test sono state visualizzate le informazioni su un host specifico per verificare a quali dischi virtuali si accedeva da VM specifiche.

Lo scopo dello scenario di test 06 è stato quello di dimostrare la conservazione di uno stato sicuro e una tolleranza ai guasti limitata in caso di guasto di un nodo. L'esecuzione del test ha dimostrato la ridondanza dell'host e la tolleranza ai guasti.

11.3 Test funzionali ed indipendenti svolti dai Valutatori

Per l'effettuazione dei test, il Fornitore ha messo a disposizione dei Valutatori un'appliance Nutanix NX-1365-G7, equivalente ad una NX-1065-G7 con 3 nodi (per maggiori informazioni fare riferimento al par. 1.6.1 del Traguardo di Sicurezza [TDS]). I Valutatori hanno seguito i passi di preparazione definiti nel documento [AGD] per creare la configurazione sicura per l'ODV. Questi includono l'aggiornamento dell'AOS alla versione 5.15 LTS, la disabilitazione dell'interfaccia IPMI, la configurazione del server NTP, la disabilitazione di SNMP e la disabilitazione del supporto remoto e la verifica della password SSH. Le versioni dell'hardware e del software sono risultate coerenti con il Traguardo di Sicurezza [TDS]. L'ODV è stato configurato seguendo passo passo il documento [AGD], che descrive come configurare l'ODV per ottenere la configurazione valutata, ed è quindi risultato coerente con il Traguardo di Sicurezza [TDS]. La documentazione di test riporta il modello esatto dell'appliance hardware, ossia NX-1365-G7, utilizzata dal Fornitore per eseguire i test funzionali, corrispondente alla stessa versione utilizzata dai Valutatori per eseguire i test.

Allo scopo di verificare i risultati dei test del Fornitore, i Valutatori hanno eseguito un campione dei test inclusi nella documentazione di test utilizzando vari strumenti (Firefox v77.0.1, Chrome v83.0.4103.116, Java SE v8 update 251, Postman v7.27.1, nCLI scaricabile da Prism). In particolare, i Valutatori hanno selezionato ed eseguito due fasi di test da ciascuno degli scenari di test definiti. I Valutatori hanno eseguito azioni quali tentativi di accesso non autorizzati e accesso con credenziali corrette, creazione ed eliminazione di VM e di container di archiviazione, ridimensionamento di dischi virtuali, tentativi di causare malfunzionamenti dell'host scollegando i nodi dalla rete.

I Valutatori sono stati in grado di riprodurre alcuni passaggi dei test scelti seguendo la documentazione di test del Fornitore. Tutti questi test hanno fornito risultati corrispondenti a quelli dei test del Fornitore.

Dopo aver esaminato gli scenari di test 01-03, i Valutatori hanno progettato nuovi test indipendenti. Pertanto, relativamente a tali casi, i Valutatori hanno selezionato un sottoinsieme del TSF per confermare che le funzioni di sicurezza operano come specificato. I Valutatori hanno prodotto la documentazione dei nuovi test progettati, eseguito i test e verificato che i risultati ottenuti fossero corrispondenti ai risultati attesi.

11.4 Analisi di vulnerabilità e test di intrusione

La prima fase della valutazione della vulnerabilità è consistita nella raccolta di informazioni sull'ODV. Come primo passo, sono state condotte varie ricerche su fonti pubbliche utilizzando diverse combinazioni di parole chiave per identificare i bug e le vulnerabilità disponibili pubblicamente per l'ODV. Per questa fase non sono stati utilizzati solo motori di ricerca, ma anche database pubblici di vulnerabilità. L'elenco delle vulnerabilità pubblicamente note è risultato piuttosto breve e composto da vulnerabilità tutte obsolete e quindi non rilevanti per l'ODV. I Valutatori hanno anche cercato ulteriore documentazione e segnalazioni di vulnerabilità nel sito Web del Fornitore e nei forum di supporto. Al termine di questa prima fase, i Valutatori hanno concluso che l'ODV è ben documentato e che un utente malintenzionato può ottenere una conoscenza approfondita dell'ODV sulla base della documentazione disponibile e delle ricerche nei forum, circostanza rilevante per il calcolo del potenziale di attacco. Ciò nonostante, non esistono vulnerabilità pubblicamente note rilevanti per l'ODV.

In una seconda fase, i Valutatori hanno utilizzato la documentazione del Fornitore per acquisire familiarità con l'ODV e per identificare le possibili superfici di attacco. Come accennato in precedenza, la documentazione disponibile pubblicamente sul sito Web del Fornitore è ricca ed è quasi corrispondente alla documentazione fornita per la valutazione. I Valutatori si sono fatti una prima opinione sull'ODV sulla base della documentazione e utilizzando le interfacce amministrative dell'ODV. Durante questa fase sono stati inoltre identificati un paio di possibili vettori di attacco alle interfacce amministrative. Poiché le interfacce amministrative dell'ODV includono un'interfaccia a riga di comando, disponibile come file eseguibile scaricabile, i Valutatori hanno anche condotto un'analisi del codice sorgente su questo eseguibile per comprenderne le funzionalità e le modalità di comunicazione con l'ODV. Tale analisi del codice sorgente ha altresì fatto emergere alcune potenziali vulnerabilità. Come risultato della seconda fase di raccolta di informazioni sono state individuate molteplici potenziali vulnerabilità, che sono state incluse nel piano dei test di intrusione.

Come ultima fase della raccolta di informazioni, i Valutatori hanno avviato una ricerca attiva di porte aperte sull'ODV installato all'interno dell'ambiente di test. Una volta identificate le porte aperte, i Valutatori hanno esaminato la documentazione ed hanno anche effettuato ricerche su ulteriori fonti pubbliche di informazioni per identificare i servizi in esecuzione dietro tali porte, in quanto la maggior parte dei servizi utilizza porte personalizzate. La ricerca ha portato come risultato alcuni post su blog in cui queste porte e servizi vengono dettagliatamente descritti. Sulla base di questi risultati, la raccolta attiva di informazioni ha portato a scoprire ulteriori potenziali vulnerabilità, che sono state incluse nel piano dei test di intrusione.

Una volta raccolte tutte le informazioni necessarie sull'ODV e sulle sue potenziali vulnerabilità, i Valutatori hanno creato un piano di test di intrusione suddiviso in diversi scenari di attacco. Per ogni scenario di attacco, è stato calcolato l'esatto potenziale di attacco, considerando il fatto che le informazioni pubblicamente disponibili sull'ODV sono molto dettagliate e ricche.

Una volta definiti gli scenari di attacco, i Valutatori hanno condotto test di intrusione sull'ODV per identificare le vulnerabilità reali. I risultati dei test sono stati documentati con un dettaglio sufficiente per consentirne la ripetibilità e i risultati sono stati raccolti in una tabella per motivi di chiarezza.

I test di intrusione eseguiti non hanno permesso di identificare vulnerabilità dell'ODV sfruttabili con potenziale di attacco Basic.

Sulla base di tali risultati, i Valutatori hanno concluso che nessuno scenario di attacco con potenziale Basic può essere completato con successo nell'ambiente operativo dell'ODV nel suo complesso. Pertanto, nessuna delle potenziali vulnerabilità identificate può essere effettivamente sfruttata. Tuttavia, i valutatori hanno identificato tre vulnerabilità residue, ovvero vulnerabilità che potrebbero essere sfruttate da un attaccante con un potenziale di attacco superiore a Basic.

Si consiglia agli utenti dell'ODV di contattare il Fornitore per ottenere ulteriori dettagli tecnici sulle vulnerabilità residue e informazioni sulle soluzioni di mitigazione.